Intelligence, politie en veiligheidsdienst

Vis, T.

Publication date:
2012

Document Version
Publisher's PDF, also known as Version of record

Intelligence, politie en veiligheidsdienst: **verenigbare grootheden?**

proefschrift

ter verkrijging van de graad van doctor
aan Tilburg University
op gezag van de Rector Magnificus,
Prof. dr. Ph. Eijlander,
volgens het besluit van het College van Decanen,
in het openbaar te verdedigen
op woensdag 6 juni 2012 om 16.15 uur

door Thijs Vis
Geboren te Delft in 1980

Promotores:
Prof.mr. T.A. de Roos
Prof.dr. H.J. van den Herik
Prof.dr. A.C.M. Spapens

Beoordelingscommissie:
Prof.mr. T. Kooijmans
Prof.dr. M.G.W. den Boer
Prof.dr. F. Bovenkerk
Prof.dr. A.B. Hoogenboom
Prof.dr. J-J. Ch. Meyer

Nederlandse Organisatie voor Wetenschappelijk Onderzoek.
Dit onderzoek is onderdeel van het IPOL-project dat is mogelijk gemaakt door NWO binnen het ToKeN-programma onder projectnummer: 634.000.435.

SIKS Dissertation Series No. 2012-22
The research reported in this thesis has been carried out under the auspices of SIKS, the Dutch Research School for Information and Knowledge Systems.

TiCC Ph.D. Series No. 22.

Omslagontwerp: Linda van Schie

ISBN/EAN: 978-90-9026783-8

Voorwoord

Dit proefschrift behandelt (1) de implementatie van de intelligencegestuurde politie (IGP) in de praktijk van de CIE en (2) de invloed daarvan op de verhouding tussen de AIVD en de CIE. Met andere woorden: ik heb de wereld van de opsporings-, inlichtingen- en veiligheidsdiensten onderzocht. Dit is een wereld die zich doorgaans lastig laat onderzoeken. De betreffende diensten doen er alles aan om de eigen activiteiten van de buitenwereld af te schermen, hetgeen veel ruimte biedt voor ongeremd speculeren en theoretiseren omtrent en dramatiseren van de betreffende organisaties en hun werkzaamheden. Dit levert soms prachtige fictie op, zoals de boeken van John le Carré of de verfilmingen van James Bond. Soms leiden de activiteiten van de organisaties tot verhitte (politieke en juridische) discussies met als inzet bijvoorbeeld de dreigende vermenging van de politie met de veiligheidsdiensten. De geheimhouding biedt echter ook bijzondere uitdagingen voor wetenschappelijk onderzoek. Want hoe onderzoek je een onderwerp dat beneveld en vertroebeld lijkt te worden door een mist van geheimhouding? Eén van de mogelijke oplossingen is door de dataverzameling te beperken tot de beschikbare openbare publicaties, bijvoorbeeld de uitgebreide juridische publicaties met betrekking tot wetgeving. Een andere oplossing is het onderzoek te richten op historische gebeurtenissen. Doorgaans geldt de operationele noodzaak tot geheimhouding voor historische onderwerpen minder sterk dan voor contemporaine onderwerpen: betrokkenen kunnen wellicht worden geïnterviewd en bepaalde informatie is gedeclassificeerd. Ik heb voor dit onderzoek echter voor een andere aanpak gekozen. Ik wilde inzicht in de actuele stand van zaken verkrijgen omtrent IGP, een concept dat door sommigen is verheven tot een paradigmawijziging, terwijl anderen het een 'achterlijk concept' noemen. Voorts wilde ik weten op welke wijze deze mogelijke paradigmawijziging de verhouding tussen het politieke inlichtingenwerk van de veiligheidsdienst AIVD en het politiële inlichtingenwerk van de CIE beïnvloedt. Is er nog sprake van een scheiding tussen beide organisaties, of is deze scheiding inmiddels (dankzij IGP) illusoir?

Onderzoeken naar criminaliteitgerelateerde onderwerpen en veiligheid gaan vaak over theoretische modellen en concepten. In veel gevallen betreft het kwantitatief onderzoek. Dit geldt ook voor onderzoeken naar de intelligencegestuurde politie. In dit onderzoek is bewust gekozen voor een min of meer etnografisch onderzoek waarbij ik een periode van twee jaar bij de politiële intelligence- en inlichtingenorganisatie heb mogen doorbrengen. Dat was een unieke belevenis. Een hoofd CIE beschreef dit erg mooi toen hij tijdens een gesprek zijn (en mijn) gedachten treffend verwoordde: "inzicht in de praktijk van het inlichtingenwerk is een demystificatie van een instituut." Tijdens het onderzoek heb ik gezien wat intelligence in de politiepraktijk daadwerkelijk inhoudt. Voorts heb ik zicht gekregen op de bijzondere uitdagingen waar de politie zich mee geconfronteerd ziet bij het implementeren van intelligence, zoals het probleem van geheimhouding van informatie, de moeilijkheid van het voorspellen van criminaliteit en de frustraties die de kop opsteken bij de politiële informatiehuishouding (de bekende ICT-problematiek). Sommige zaken beantwoordden aan mijn beeld, maar voor het grootste deel heb ik mijn beeld moeten bijstellen. Van tevoren had ik het idee dat het vanwege de verregaande geheimhouding bijzonder lastig zou zijn om zicht te krijgen op de praktijk van IGP en de verhouding tussen de AIVD en de CIE. Dat bleek in de praktijk echter bijzonder mee te vallen. Diverse (voormalige) medewerkers van de AIVD bleken de tijd en mogelijkheid te hebben voor een interview en waren, voor

zover valt te beoordelen, openhartig. Het onderzoek riep ook nieuwe vragen op. Tijdens de interviews en de rest van de dataverzameling vielen twee dingen op, te weten de rol van vertrouwen in de onderlinge interactie en de rol van geheimhouding als storende factor voor het vertrouwen. Iedereen spreekt over vertrouwen, het uitwisselen van informatie en samenwerken, maar wat deze begrippen inhouden en, belangrijker nog, wat ze in de praktijk van de politiek- en politiële inlichtingen betekenen en hoe bijvoorbeeld vertrouwen kan worden gerealiseerd, is doorgaans een raadsel. Dit onderzoek bood me de kans om deze begrippen te onderzoeken en uit te werken voor de intelligence-praktijk.

Ik geef graag toe dat een ding bijzonder veel indruk op me heeft gemaakt: de saamhorigheid binnen de politieorganisatie. Ik heb een mate van collegialiteit ervaren die ik elders nergens ben tegengekomen. Daarom wil ik hier allereerst de medewerkers van de AIVD en politie bedanken die ik in mijn onderzoeksperiode heb ontmoet. Zij hebben een onuitwisbare indruk op mij achtergelaten en ik zal ze dan ook zeker niet vergeten. Meer specifiek wil ik hier (in willekeurige volgorde) Marja, Curd, Peter en Hans bedanken. Zonder jullie hulp en input was dit proefschrift er niet gekomen, althans niet zoals het er nu ligt. Voorts gaat mijn bijzondere dank uit naar de diverse leidinggevenden die hun nek hebben uitgestoken en het lef hadden om een externe onderzoeker binnen te halen en alle mogelijke medewerking te bieden. Dat alleen al laat zien dat veel van de verhalen omtrent 'geheime diensten' meer op perceptie dan op empirische feiten berust.

Graag wil ik op deze plek ook de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) en de Raad van de Rechtspraak bedanken voor de financiering van het onderzoek. De faculteit der Rechtsgeleerdheid, departement Strafrecht en Criminologie van de Universiteit Leiden, de faculteit der Rechtsgeleerdheid, departement Strafrechtswetenschappen van *Tilburg University*, het *Tilburg Center for Cognition and Communication* (TICC) en de Nederlandse Onderzoeksschool voor Informatie- en Kennissystemen SIKS bedank ik voor het faciliteren van het onderzoek.

Ook Linda ben ik erg dankbaar voor alle hulp bij de opmaak en uiteindelijke vormgeving.

Tot slot wil ik mijn vriendin Tannie bedanken voor haar steun, motivatie en eindeloze geduld. De afgelopen zes jaar stonden voor haar tegen wil en dank in het teken van de wetenschap.

Thijs Vis

Utrecht, juni 2012

Nagekomen: nadat de tekst van het proefschrift was afgerond en het proefschrift was goedgekeurd door de beoordelingscommissie kwam de publicatie "*Het toezicht op de inlichtingen en veiligheidsdiensten: de noodzaak van krachtiger samenspel*" van Cyrille Fijnaut uit. Om dit werk een plaats te geven in dit proefschrift heb ik een voetnoot opgenomen (voetnoot 154). De inhoud van dat werk is evenwel niet verder in het proefschrift verwerkt. Voorts is ook de val van het kabinet Rutte op 23 april 2012 vanwege de mogelijke invloed op de vorming van de nationale politie relevant voor ons proefschrift. Ook hiervoor geldt dat het niet in het proefschrift is verwerkt.

Inhoudsopgave

VOORWOORD - i -

INHOUDSOPGAVE - iii -

LIJST VAN AFKORTINGEN - x -

1| INLEIDING - 1 -

1.1 Aanleiding van het onderzoek - 1 -

1.1.1 Het ontstaan van IGP - 2 -

1.1.2 IGP in Nederland - 3 -

1.2 Intelligence: grondbegrippen en definities - 3 -

1.3 De scheiding van de veiligheidsdiensten en de politie - 7 -

1.3.1 Het Engelse model - 7 -

1.3.2 Het Franse model - 8 -

1.4 De Nederlandse scheiding tussen de AIVD en de politie - 8 -

1.5 Vanaf 1990: veiligheidsdiensten op zoek naar een nieuwe markt - 9 -

1.6 Vanaf 2000: terrorisme als nieuwe markt voor de politie - 10 -

1.6.1 Het primaat van de terrorismebestrijding - 11 -

1.6.2 Drie veranderingen bij de terrorismebestrijding - 12 -

1.6.3 Gevolgen voor de verhouding - 13 -

1.7 Kritiek op een mogelijke vermenging van de AIVD en de politie - 14 -

1.8 Probleemstelling en onderzoeksvragen - 15 -

1.9 Onderzoekskeuze voor de term 'bestrijding' - 17 -

1.10 De onderzoekskeuze voor de CIE, georganiseerde criminaliteit en terrorisme - 18 -

1.11 De onderzoekskeuze voor Angelsaksische literatuur - 21 -

1.12 Onderzoeksmethode - 22 -

1.12.1 Exploratief empirisch onderzoek - 22 -

1.12.2 Etnografisch onderzoek - 23 -

1.12.3 Methode van dataverzameling 1: literatuuronderzoek - 25 -

1.12.4 Methode van dataverzameling 2: veldwerk - 26 -

1.13 Structuur van het proefschrift - 27 -

2| ALGEMENE KENMERKEN VAN VEILIGHEIDSDIENSTEN EN DE POLITIE - 29 -

2.1 HP-kenmerk 1: het beschermen van de nationale veiligheid - 30 -

2.2 HP-kenmerk 2: voorwaarschuwingen en proactief signaleren van bedreigingen - 33 -

2.3 HP-kenmerk 3: de intelligence-cyclus - 36 -

2.4 Kritiek op de intelligence-cyclus - 43 -
2.5 Ons aangepast model - 44 -
2.6 HP-kenmerk 4: geheimhouding - 45 -
2.6.1 Geheimhouding in het algemeen - 46 -
2.6.2 Redenen voor geheimhouding - 46 -
2.6.3 Problematische elementen van geheimhouding - 49 -
2.7 De politie - 50 -
2.8 LP-kenmerk 1: handhaving van de rechtsorde - 51 -
2.9 LP-kenmerk 2: de strafprocesrechtelijke waarheidsvinding - 53 -
2.10 LP-kenmerk 3: opsporingsonderzoek - 55 -
2.11 LP-kenmerk 4: transparantie - 57 -
2.12 Hoofdstukconclusie: antwoord OV 1 - 58 -
3| DE ALGEMENE INLICHTINGEN- EN VEILIGHEIDSDIENST - 61 -
3.1 Organisatie van de AIVD - 61 -
3.2 De activiteiten van de AIVD - 62 -
3.2.1 De functie en taak volgens de WIV 2002 - 63 -
3.2.2 Nationale veiligheid - 64 -
3.2.3 Het 'nationale' van nationale veiligheid - 65 -
3.2.4 De A-taak - 66 -
3.2.5 Terrorisme - 67 -
3.3 Informatieverzameling - 73 -
3.3.1 De algemene bevoegdheid van art. 17 WIV 2002 - 74 -
3.3.2 De bijzondere bevoegdheden - 76 -
3.3.3 Subsidiariteit - 76 -
3.3.4 Proportionaliteit - 77 -
3.3.5 Praktijk en procedures - 77 -
3.3.6 HUMINT: het runnen van agenten door de AIVD - 79 -
3.3.7 Wat doet een agent? - 80 -
3.3.8 De agent en strafbare feiten - 81 -
3.4 Informatieverwerking - 82 -
3.4.1 Interne gegevensverstrekking - 83 -
3.4.2 De externe gegevensverstrekking: gesloten verstrekkingsregime - 84 -
3.5 AIVD-informatie in het strafproces - 87 -
3.6 De RID - 88 -

3.6.1 De AIVD-taak van de RID - 88 -
3.6.2 De RID en de opsporing - 90 -
3.6.3 De openbare orde taak van de RID - 90 -
3.7 De politiek-bestuurlijke context van de AIVD - 92 -
3.7.1 Sturing - 92 -
3.7.2 De Commissie van toezicht op de Inlichtingen- en Veiligheidsdiensten - 94 -
3.8 Hoofdstukconclusie: antwoord OV 1 - 96 -
4| DE CRIMINELE INLICHTINGENEENHEID - 99 -
4.1 Historische ontwikkeling CIE - 99 -
4.2 De CIE in het algemeen - 106 -
4.2.1 Waarom een CIE? - 107 -
4.2.2 De taak en de werkzaamheden van de CIE - 107 -
4.2.3 De afscherming van de identiteit van de informant - 110 -
4.2.4 Organisatie - 111 -
4.3 Verzamelen - 112 -
4.3.1 Juridische basis: artikel 2 Politiewet - 113 -
4.3.2 Juridische basis: artikel 126v WvSv - 114 -
4.3.3 Een informant als verdachte - 118 -
4.3.4 Runnen in de praktijk - 120 -
4.3.5 Runnen exclusief door de CIE - 120 -
4.4 Verwerken - 121 -
4.4.1 De Wet Politiegegevens als juridische grondslag - 122 -
4.4.2 Artikel 12-verwerkingen - 123 -
4.4.3 Zwacri-verwerkingen van artikel 10 lid 1 sub a WPG - 125 -
4.4.4 Terrorisme: themaverwerking - 127 -
4.5 Verstrekken - 128 -
4.5.1 Verstrekking uit artikel 12-domein - 129 -
4.5.2 Verstrekking uit het artikel 10-domein - 131 -
4.5.3 Verstrekkingen aan de AIVD - 132 -
4.6 Hoofdstukconclusie - 134 -
5| DE INTELLIGENCEGESTUURDE POLITIE - 139 -
5.1 Historische ontwikkelingen - 139 -
5.1.1 Community policing - 140 -
5.1.2 De probleemgestuurde politie - 141 -

5.2 Nieuwe ontwikkelingen - 142 -
5.2.1 Effectiviteit en efficiency - 142 -
5.2.2 Opkomst georganiseerde criminaliteit - 144 -
5.2.3 De opkomst van terrorisme - 144 -
5.2.4 Schaalvergroting - 145 -
5.3 Theoretische verklaringen voor IGP - 146 -
5.3.1 Concept A: De risicomaatschappij - 147 -
5.3.2 Concept B: Surveillance - 148 -
5.4 IGP - 149 -
5.4.1 Verwerken van informatie: de informatiepositie - 151 -
5.4.2 Proactieve werkwijze en preventieve criminaliteitsbestrijding - 151 -
5.4.3 Effectieve sturing - 152 -
5.4.4 Delen van informatie - 153 -
5.4.5 IGP: oude wijn in nieuwe zakken? - 153 -
5.4.6 Ratcliffe's 3i-model - 154 -
5.4.7 Intelligence - 155 -
5.5 Twee uitwerkingen van IGP in Nederland - 158 -
5.5.1 ABRIO - 159 -
5.5.2 Het NIM - 160 -
5.6 Nieuwe begrippen en nieuwe analyses - 168 -
5.6.1 HP-kenmerk 2: voorwaarschuwing - 169 -
5.6.2 HP-kenmerk 3: de intelligence-cyclus - 170 -
5.6.3 HP-kenmerk 4: geheimhouding - 171 -
5.7 Hoofdstukconclusie en antwoord op OV 2 - 172 -
6| HET PRAKTIJKONDERZOEK - 175 -
6.1 Opzet van het onderzoek - 175 -
6.2 Dataverzameling in de praktijk - 176 -
6.2.1 Het literatuuronderzoek - 176 -
6.2.2 De participerende observatie - 176 -
6.2.3 De interviews - 178 -
6.2.4 De ('grijze') literatuur - 181 -
6.3 De analyse van de data - 182 -
6.4. Afspraken en geheimhouding - 183 -
6.5 Het veldwerk - 183 -

6.5.1 De eerste indruk: demystificatie van een instituut - 184 -
6.5.2 Acceptatie - 186 -
6.5.3 Een dynamische omgeving? - 189 -
6.5.4 Tot slot: *Going native?* - 191 -
7| IGP IN DE PRAKTIJK - 195 -
7.1 Wat is IGP? - 195 -
7.1.1 Onduidelijkheid omtrent IGP - 196 -
7.1.2 IGP als informatieproduct (de product-benadering) - 199 -
7.1.3 IGP als voorwaarschuwing (de intelligence-benadering) - 200 -
7.1.4 Tussenconclusies - 201 -
7.2 Sturing in de praktijk - 201 -
7.2.1 De strategische sturing - 202 -
7.2.2 Dilemma's van operationele en tactische sturing - 211 -
7.2.3 Tussenconclusies - 215 -
7.3 Verzamelen van informatie in de praktijk - 216 -
7.3.1 Proactieve informatieverzameling - 217 -
7.3.2 Gerichte informatieverzameling - 221 -
7.3.3 Tussenconclusies - 223 -
7.4 Verwerken van informatie in de praktijk - 223 -
7.4.1 Informanten-informatie - 223 -
7.4.2 Rest- en zijtak-informatie - 231 -
7.4.3 Tussenconclusies - 233 -
7.5 Analyse in de praktijk - 234 -
7.5.1 Operationele en tactische analyse - 234 -
7.5.2 Strategische analyse - 237 -
7.5.3 De traditionele recherchefunctie versus de nieuwe informatiefunctie - 243 -
7.5.4 Tussenconclusies - 245 -
7.6 Verstrekken in de praktijk: de intra-organisatorische geheimhouding - 246 -
7.6.1 Doelstelling 1: *Need to share* bij de CIE - 247 -
7.6.2 Doelstelling 2: *old boys networks* - 255 -
7.6.3 Tussenconclusies - 258 -
7.7 Hoofdstukconclusie en antwoord op OV 3 - 259 -
8| DE AIVD EN DE CIE: EEN MOEIZAME RELATIE - 263 -
8.1 De traditionele conceptuele verhouding tussen de AIVD en de politie - 263 -

8.2 Veranderingen - 264 -
8.2.1 Verandering in taak - 265 -
8.2.2 Verandering in middel - 268 -
8.2.3 Veranderingen in het werkproces - 273 -
8.2.4 Veranderingen in de relatie met externen? - 273 -
8.2.5 Tussenconclusie - 274 -
8.3 Vertrouwen - 276 -
8.3.1 Onderling vertrouwen volgens respondenten - 276 -
8.3.2 Het concept 'vertrouwen' - 277 -
8.4 Kenmerk 1: de driehoeksrelatie - 279 -
8.4.1 Traditionele afstemming en communicatie - 280 -
8.4.2 Een hiërarchische verhouding - 281 -
8.5 Kenmerk 2: De reden voor vertrouwen (*incentive*) - 283 -
8.6 Kenmerk 3: Risico - 284 -
8.7 Conclusie: is er sprake van vertrouwen? - 286 -
8.8 De RID - 287 -
8.9 Afstemming en overleg door middel van het AOT/IOT - 289 -
8.10 Stelselmatige informatie-uitwisseling - 293 -
8.11 Samenwerking in het kader van de CT-infobox - 298 -
8.12 Hoofdstukconclusie en antwoord op OV4 - 303 -
9| CONCLUSIES - 307 -
9.1 De conceptuele verhouding tussen de AIVD en de CIE - 307 -
9.2 Het concept IGP - 312 -
9.3 IGP in de praktijk - 313 -
9.3.1 Algemene barrières voor een succesvolle implementatie van IGP - 314 -
9.3.2 De implementatie van het NIM binnen de CIE - 317 -
9.3.3 Concluderend - 321 -
9.4 De verhouding tussen de AIVD en de CIE - 322 -
9.4.1 Verschuivingen in de conceptuele verhouding - 322 -
9.4.2 De interactie en de rol van vertrouwen - 323 -
9.4.3 De interactie in de praktijk - 324 -
9.5 Antwoord op de centrale probleemstelling - 325 -
9.5.1 Verschuivingen in de verhouding? - 325 -
9.5.2 Causaal verband? - 327 -

9.6 Discussie - 328 -
9.6.1 De barrières tegen IGP - 329 -
9.6.2 De verhouding tussen de AIVD en de CIE - 337 -
9.7 Slotbeschouwing - 345 -
SAMENVATTING - 347 -
SUMMARY - 353 -
REFERENTIES - 359 -
CURRICULUM VITAE - 381 -
SIKS DISSERTATION SERIES - 383 -

Lijst van afkortingen

ABRIO – Aanpak Bedrijfsvoering Recherche, Informatie en Opleiding

AIVD – Algemene Inlichtingen en Veiligheidsdienst

AMvB – Algemene Maatregel van Bestuur

Wet BIBOB – Wet Bevordering Integriteitsbeoordelingen door het Openbaar Bestuur

Bpolg – Besluit Politiegegevens

BVD – Binnenlandse Veiligheidsdienst

BVO – Basisvoorziening Opsporing

CAPPS – *Computer Assisted Passenger Prescreening System*

CBA - Criminaliteitsbeeldanalyse

CBB – Coördinator Bewaken en Beveiligen

CBP – College Bescherming Persoonsgegevens

CIA – *Central Intelligence Agency*

CIE – Criminele Inlichtingen Eenheid

CPN – Communistische Partij Nederland

CSV – Crimineel Samenwerkingsverband

CT-infobox – Contra Terrorisme Informatiebox

CTIVD – Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

CVIN – Comité Verenigde Inlichtingendiensten Nederland

DCRG – *Direction central des renseignements généraux*

DCRI - *Direction Centrale du Renseignement Intérieur*

DEA – *Drug Enforcement Agency*

DIK – Districtelijk Informatie Knooppunt

DNR – Dienst Nationale Recherche

DRIO – Dienst Regionale Informatie Organisatie (zie ook: RIO)

DST – *Direction de la Surveillance du Territoire*

EHRM – Europees Hof voor de Rechten van de Mens

EVRM – Europees Verdrag voor de Rechten van de Mens

FARC - Fuerzas Armadas Revolucionarias de Colombia–Ejército del Pueblo

(Revolutionaire Strijdkrachten van Colombia)

FBI – *Federal Bureau of Investigation*

FIOD – Fiscale Inlichtingen- en Opsporingsdienst

GBA – Gemeentelijke Basis Administratie

Gestapo – *Geheime Staatspolizei*

HP – *High Policing*

HUMINT – *Human Intelligence*

IDB – Inlichtingendienst Buitenland

IGO – Informatiegestuurde Opsporing

IGP – Intelligencegestuurde Politie

ILP – *Intelligence Led Policing*

IND – Immigratie- en Naturalisatie Dienst

IOOV - Inspectie Openbare Orde en VeiligheidIOT – Inlichtingen Overleg Terrorisme

IRA – *Irish Republican Army*

IVD – Inlichtingen- en veiligheidsdienst

KLPD – Korps Landelijke Politiediensten

KIM – Kennis in Modellen

Kmar – Koninklijke Marechaussee

LIK – Landelijk Informatie Knooppunt

LP – *Low Policing*

LPC – Landelijk Platvorm CIE-officieren

LPF – Lijst Pim Fortuyn

MI5 – *Military Intelligence Section 5*

MID – Militaire Inlichtingendienst

MIVD – Militaire Inlichtingen- en Veiligheidsdienst

MvT – Memorie van Toelichting

NBCR-terrorisme – Nucleair, Biologisch, Chemisch en Radioactief terrorisme

NCTb – Nationaal Coördinator Terrorismebestrijding

NCTV – Nationaal Coördinator Terrorismebestrijding en Veiligheid

NDB – Nationaal Dreigingsbeeld

NIM – Nationaal Intelligence Model

NSA – *National Security Agency*

OM – Openbaar Ministerie

OSINT – *Open Source Intelligence*

OvJ – Officier van Justitite

PKK - *Partiya Karkerên Kurdistan* (arbeiderspartij Koerdistan)

PV – Proces-verbaal

RID – Regionale Inlichtingendienst

RIK – Regionaal Informatie Knooppunt

RIO – Regionale Informatie Organisatie

RT-pijler – Radicaliseringstendensen-pijler

RvHC – Raad van Hoofdcommissarissen

SGBO – Staf Grootschalig Bijzonder Optreden

SIGINT – *Signal Intelligence*

Stasi - *Ministerium für Staatssicherheit*

Vedomi – Verdovende middelen

VtSPN – Voorziening tot Samenwerking Politie Nederland

WBP – Wet Bescherming Persoonsgegevens

Wet BOB – Wet Bijzondere Opsporingsbevoegdheden

WIV – Wet op de Inlichtingen en Veiligheidsdiensten

WPG – Wet Politiegegevens

WvSv – Wetboek van Strafvordering

ZIR - Zwacri informatierapport

Zwacri – Zware Criminaliteit

1| Inleiding

In dit onderzoek behandelen wij twee zaken die nauw met elkaar zijn verweven. Het gaat om (1) de wijze waarop de Nederlandse politie het concept 'intelligencegestuurde politie' (verder IGP)[1] implementeert en heeft geïmplementeerd in de context van de Criminele Inlichtingeneenheid (CIE) en (2) in hoeverre deze implementatie van invloed is op de verhouding tussen de CIE en de Algemene Inlichtingen en Veiligheidsdienst (AIVD). Op grond van rechtsstatelijke overwegingen zijn de AIVD en de politie immers van elkaar gescheiden. IGP is echter deels afkomstig uit de wereld van de inlichtingen- en veiligheidsdiensten. Dit betekent dat de implementatie van IGP in een politiële context mogelijk kan leiden tot het loslaten van deze scheiding. Het doel van dit onderzoek is vast te stellen in hoeverre het concept IGP in de politiële inlichtingenpraktijk is geïmplementeerd en wat de invloed van deze implementatie is op de verhouding tussen de AIVD en de politie.

In sectie 1.1 schetsen wij de aanleiding van dit onderzoek. Daar behandelen wij ook kort de achtergrond van IGP bij de politie. Sectie 1.2 behandelt het begrip intelligence en geeft de definities die wij in dit onderzoek gebruiken. Vervolgens beschrijft sectie 1.3 de scheiding tussen de (inlichtingen- en) veiligheidsdiensten en de politie aan de hand van twee modellen. Zo krijgt de lezer inzicht in ten minste twee manieren waarop de scheiding kan worden georganiseerd. Sectie 1.4 werkt de scheiding tussen de veiligheidsdiensten en de politie verder uit voor de Nederlandse situatie. In sectie 1.5 staat de 'nieuwe markt' die de inlichtingen- en veiligheidsdiensten na het wegvallen van de Sovjet-Unie hebben gevonden centraal, te weten de bestrijding van de georganiseerde criminaliteit. Sectie 1.6 beschrijft vervolgens de opkomst van terrorisme als 'nieuwe markt' voor de politie na 11 september 2001. Niet onverwachts leidt de vermeende toenemende vermenging van de politie met de veiligheidsdiensten tot kritiek. Dit is het onderwerp van sectie 1.7. We zijn nu bij het hoofdpunt van dit onderzoek aangekomen: de probleemstelling en de hoofdvragen. Zij worden in sectie 1.8 geformuleerd. In de secties 1.9, 1.10 en 1.11 verantwoorden wij achtereenvolgens onze keuzes voor het gebruik van de term 'bestrijding' (1.9), de afbakening van het onderzoek tot georganiseerde criminaliteit en terrorisme (1.10) en voor het veelvuldig gebruik van Angelsaksische literatuur (1.11). In sectie 1.12 behandelen wij de door ons gehanteerde onderzoeksmethode en de methoden van dataverzameling. Tenslotte geeft sectie 1.13 een overzicht van de structuur en opbouw van het boek.

1.1 Aanleiding van het onderzoek

Sinds de jaren '90 van de vorige eeuw is er een nieuwe 'politiehype' opgedoken in de vorm van IGP (Gill 2000; Ratcliffe 2008). Nu duikt er in het politiebestel wel vaker een concept op dat het politieland snel lijkt te veroveren. Het gaat dan meestal om concepten die direct inspelen op een bepaalde algemene trend in de samenleving. De politie reageert daar vervolgens op. Zo is er veel geld gestoken in het ontwikkelen en

[1] Wij gebruiken in dit boek het Engelse woord *intelligence* in een Nederlandse context. Vanaf nu beschouwen wij het woord 'intelligence' als een Nederlands woord en zullen het niet gaan cursiveren of tussen *single quotes* plaatsen. In sectie 1.2 gaan wij verder in op de betekenis en de rol van intelligence.

implementeren van eerdere concepten als *community policing* en de probleemgestuurde politie, en nu herhaalt dit zich met betrekking tot IGP. In ons onderzoek analyseren wij zoals gezegd (1) of de implementatie van IGP het politiële inlichtingenwerk daadwerkelijk heeft veranderd en (2) in hoeverre de genoemde ontwikkeling de verhouding tussen de CIE van de politie en de AIVD heeft beïnvloed of nog beïnvloedt. Daartoe behandelen wij in subsectie 1.1.1 eerst kort het ontstaan van het concept IGP in het algemeen en vervolgens in subsectie 1.1.2 IGP in Nederland in het bijzonder. Deze onderwerpen komen in hoofdstuk vijf uitgebreid aan bod. Het gaat er op dit moment echter om een beeld te schetsen dat naar het hoofdpunt van de studie leidt: de probleemstelling en de onderzoeksvragen.

1.1.1 Het ontstaan van IGP

IGP heeft volgens de 'politielegende' haar oorsprong in Kent, Groot-Brittannië in het begin van de jaren '90. Dit nieuwe concept was onder meer een reactie op de toenemende kritiek op het functioneren van de politiediensten aldaar (zie Gill 2000; Ratcliffe 2008). De geregistreerde criminaliteit nam jaar op jaar toe en de politie leek hier niets aan te (kunnen) doen. De politie zou verouderde reactieve opsporingsmethoden hanteren die weinig effectief waren in de bestrijding van criminaliteit. Zij moest, dacht men toen, proactiever te werk gaan en zoveel mogelijk proberen criminaliteit te voorkomen, onder andere door zich specifiek te richten op veelplegers die verantwoordelijk waren voor veel criminaliteit. Indien de politie niet zou veranderen van een reactieve organisatie naar een proactieve organisatie, dan zouden bezuinigingen en andere (financiële) maatregelen niet uitgesloten geacht moeten worden (Gill 2000; Ratcliffe 2008). Het was voor het eerst in de Britse geschiedenis dat de politie zich geconfronteerd zag met zoveel kritiek en mogelijke bezuinigingen. Voor de Britse politie zat er niets anders op dan haar eigen functioneren fundamenteel te herzien, maar de vraag was hoe ze dat zou moeten doen. Het is immers niet niks om een politiebestel volledig te hervormen. Bureaucratieën zijn notoir log als het gaat om het doorvoeren van veranderingen, niet in de laatste plaats omdat veel medewerkers in die organisaties helemaal niet zitten te wachten op verandering (zie Lipsky 1980; Benveniste 1998). Daarnaast moet er sprake zijn van een concept en een visie volgens welke de organisatie daadwerkelijk kan worden hervormd (Maesschalck 2008: 4). Verder is de vraag relevant of de politie daadwerkelijk iets kan doen aan de toenemende criminaliteit. Dit zijn lastige onderwerpen en vragen waar het regionale politiekorps van Kent, Groot Brittannië, in de jaren '90 een antwoord op leek te hebben gevonden.

Medewerkers van het politiekorps van Kent kwamen op het idee om de criminaliteitsinformatie die al aanwezig was in de politieorganisatie bijeen te brengen en te analyseren om zo de kenmerken en dynamiek van de criminaliteit bloot te leggen (zie Gill 2000; Ratcliffe 2008). Met behulp van de geanalyseerde informatie kunnen onder andere veelplegers en *hotspots* worden geïdentificeerd. Deze inzichten zouden het mogelijk moeten maken de politie gerichter aan te sturen en de politiële inzet te focussen op deze veelplegers en *hotspots*. De nieuwe aanpak zou de politie effectiever en efficiënter maken. Het concept kreeg de naam *intelligence led policing* (ILP). Daarmee had de Britse politie een concept in handen waarmee ze proactief kon worden en waarmee ze iets tegenover de critici van de politie kon plaatsen. Het concept werd al snel overgenomen door andere politiediensten en werd met name toegepast bij de opsporing van de zware en georganiseerde criminaliteit. Onder de noemer *National Intelligence Model* (NIM) werd in 2000 het (gehele) Britse

opsporingsproces gereorganiseerd volgens de principes van IGP (Ratcliffe 2008: 38-39). Na de invoering van het concept claimden de Britse korpsen succes na succes, hetgeen overheden en politiediensten in het buitenland niet ontging. Ook buiten Groot-Brittannië werden politiekorpsen vanaf die tijd geconfronteerd met de maatschappelijke eis en structurele wens om proactief te werk te gaan. Dit gold eveneens voor Nederland.

1.1.2 IGP in Nederland

De Nederlandse politie omarmde omstreeks 2000 IGP als het nieuwe antwoord op de criminaliteitsproblematiek (zie De Hert, Huisman en Vis 2005). In eerste instantie werd het 'de informatiegestuurde opsporing' genoemd, oftewel IGO. IGO is later omgevormd tot IGP: het begrip informatie werd vervangen door het begrip intelligence, en het begrip opsporing werd vervangen door het bredere begrip politie. Het moest zowel de opsporing als het overige politiewerk grondig hervormen. In 1996 werd in Nederland de stuurgroep ABRIO (Aanpak Bedrijfsvoering Recherche, Informatie en Opleiding)[2] ingesteld die aan het begin van deze eeuw de opdracht kreeg allereerst te onderzoeken of het Nederlandse politiebestel klaar was voor de invoering van IGP en, indien dit niet het geval was, wat er aan gedaan kon worden om dit wel mogelijk te maken (zie Jansen 2001). Inmiddels (2011) lijkt ieder onderdeel van de politie het concept IGP te hebben omarmd: het is een politiebrede ontwikkeling geworden. Dit blijkt ook uit het streven van de Raad van Hoofdcommissarissen om de gehele Nederlandse politie vanaf 2012 volgens IGP te laten werken.[3]

Net als haar voorgangers wordt IGP gepresenteerd als hèt antwoord op de problematiek bij de politie. Sommigen noemen het zelfs een nieuw paradigma voor het politiewerk (Ratcliffe 2008). De recente opkomst van terrorisme heeft de ontwikkeling van IGP daarbij nog een stevige nieuwe impuls gegeven; bij de bestrijding van terrorisme is de noodzaak voor proactiviteit immers het grootst. De politie zal aanslagen moeten voorkomen en niet kunnen afwachten totdat een aanslag plaatsvindt en dan pas optreden.[4] IGP lijkt in deze behoefte voor proactivering van het politiewerk te kunnen voorzien.

Inmiddels wordt het concept in vrijwel de gehele westerse wereld over de politiediensten uitgerold en krijgt het een steeds bredere toepassing. Over de precieze definitie van intelligence, lopen de meningen echter uiteen. In de volgende sectie geven wij onze definitie.

1.2 Intelligence: grondbegrippen en definities

Het kernbestanddeel van IGP is intelligence. Intelligence zorgt er voor dat IGP als een grote verbetering van het traditionele politiewerk wordt gezien. In deze sectie staan wij daarom kort stil bij wat intelligence is en geven wij zeven definities die van belang zijn voor dit onderzoek.

---

[2] Deze stuurgroep viel onder de Raad van de Hoofdcommissarissen. Inmiddels bestaat ABRIO niet meer. Het programma is echter voortgezet in (1) het Programma Innovatie Opsporing, oftewel PIO en in (2) meerdere regiogebonden stuur- en werkgroepen.

[3] De RvHC heeft dit doel in het kader van het Nationaal Intelligence Model (NIM 2008) vastgesteld.

[4] Dit is met name in de VS het geval. Zonder de aanslagen van 9-11 zou IGP daar waarschijnlijk nooit zo belangrijk zijn geworden als het vandaag de dag is. Zie: Ratcliffe (2008); Mc Garell, Freilich en Chermak (2007).

Intelligence is een verwarrende term omdat er veel verschillende definities voor worden gebruikt (zie Warner 2002). Sommigen kiezen voor een letterlijke vertaling naar het Nederlands en zien intelligence als een vorm van inlichtingen (Van der Bel, van Hoorn en Pieters 2009). Anderen zien het als een modaliteit van informatie: intelligence is dan geanalyseerde en actiegericht gemaakte informatie (zie Meesters en Niemeijer 2000; Minnebo 2004; zie ook subsectie 5.3.7).

De huidige definities schieten naar onze mening tekort omdat ze òf te specifiek gericht zijn op een bepaalde soort van informatie, òf ze te breed zijn zodat ze geen onderscheidend kenmerk hebben ten opzichte van andere soorten van informatie (De Hert, Huisman en Vis 2005). Een begrip als intelligence moet kenmerken hebben waardoor het zich onderscheidt van andere vergelijkbare begrippen. Zo niet, dan valt het begrip intelligence lastig te analyseren, laat staan te implementeren. Immers, als iets veel omvattend is, op welk element dient een onderzoeker, een uitvoerder of de gehele politieorganisatie zich dan te richten? Als intelligence bijvoorbeeld een vorm van geanalyseerde en actiegerichte informatie is, dan zouden bewijsmiddelen ook onder de noemer intelligence kunnen worden geschaard. Dit is zowel onwenselijk als onjuist. Allereerst is het onwenselijk om het begrip te breed te definiëren omdat het begrip daardoor diffuus en onduidelijk wordt. Daarnaast is het onjuist om bewijsmiddelen onder intelligence te scharen, omdat intelligence binnen de politieorganisatie gezien dient te worden als iets nieuws, als een verbetering ten opzichte van de traditionele politie met haar reactieve werkwijze en focus op de opsporing. In die traditionele politieorganisatie is het bewijsmiddel als reactieve modaliteit van informatie van groot belang, bewijsmiddelen zijn immers per definitie gericht op het verleden (het gaat bij de opsporing om materiële waarheidsvinding hetgeen noodzakelijkerwijs het verleden betreft, zie sectie 2.9). Het zal duidelijk zijn: zowel de praktijk als de wetenschap is geholpen bij een heldere, afgebakende definitie. Dit brengt ons op de definitie die wij zullen hanteren.

Om te begrijpen wat intelligence nu zo aantrekkelijk maakt voor de politie, is het wellicht verstandig om te rade te gaan bij de herkomst van het begrip. Intelligence is namelijk de naam voor het werkproces van inlichtingendiensten, die niet voor niets in het Engels ook wel *intelligence agencies* worden genoemd. Wanneer we naar de definitie van intelligence voor de inlichtingen- en veiligheidsdiensten kijken, komen we uit bij de definitie van Gill en Phythian (2006). Zij definiëren intelligence als een concept en geven in de definitie duidelijk aan wat intelligence anders maakt dan andere modaliteiten van informatie. Daarmee wordt duidelijk wat intelligence aantrekkelijk maakt voor de opsporingspraktijk. Wij hanteren daarom de volgende definitie van intelligence.

Definitie 1: Intelligence is de overkoepelende term voor de reeks van activiteiten – van het vaststellen van een inlichtingenbehoefte en het verzamelen van informatie tot analyse en verspreiding – die in het geheim plaatsvinden en die zijn gericht op het bewaken of vergroten van veiligheid door middel van het geven van voorwaarschuwingen voor bedreigingen of potentiële bedreigingen op een manier die ruimte biedt voor een tijdige implementatie van een preventief beleid of strategie (…).[5]

[5] De oorspronkelijke Engelstalige definitie van Gill en Phythian luidt als volgt: "*(Intelligence is) the umbrella term referring to the range of activities- from planning and information collection to analysis and dissemination- conducted in secret, and aimed at maintaining or enhancing relative security by providing forewarning of threats or potential threats in a manner that allows for the timely implementation of a preventive policy or strategy (…)*" (Gill en Phythian 2006: 7).

Deze definitie ziet intelligence (1) als product, (2) als proces en (3) als verzameling van missies/taken. De meerwaarde van intelligence is dat het een voorwaarschuwing van een dreiging geeft. Inlichtingen- en veiligheidsdiensten hebben als taak het beschermen van de nationale veiligheid, en moeten ingrijpen voordat een bedreiging van die nationale veiligheid werkelijkheid wordt. Al hun inspanningen en werkprocessen zijn er dan ook op gericht om bedreigingen tijdig te onderkennen en de uitvoering ervan zoveel mogelijk te voorkomen. In tegenstelling tot de traditionele politie gaat het inlichtingen- en veiligheidsdiensten dus niet zozeer om wat er in het verleden is gebeurd, maar met name om wat er nog staat te gebeuren. Met andere woorden, de traditionele politie kijkt terug en richt zich op het verleden terwijl de inlichtingen- en veiligheidsdiensten vooruit kijken en zich richten op het heden en met name op de toekomst. De door de inlichtingen- en veiligheidsdienst gebruikte intelligence-processen zijn dan ook vanwege de toenemende nadruk binnen de samenleving op criminaliteitspreventie en risicocontrole voor de politie erg interessant (zie ook Ratcliffe 2008: 18).[6] Het is derhalve niet verwonderlijk dat de politie juist intelligence heeft gekozen als reactie op de grote uitdagingen waarmee zij sinds de jaren '90 van de vorige eeuw is geconfronteerd.[7]

Bij de preventieve doelstellingen van intelligence hoort ook een proactieve benadering van de informatieverzameling. De door de intelligence diensten heimelijk verzamelde informatie definiëren wij als 'inlichtingen'.

Definitie 2: Inlichtingen zijn informatie items die heimelijk en proactief, dat wil zeggen op eigen initiatief, zijn verzameld.

Intelligence heeft als doelstelling preventie door middel van het geven van voorwaarschuwingen en gaat uit van een proactieve werkwijze door middel van het verzamelen van inlichtingen. Zowel preventie als proactiviteit maken het incorporeren van intelligence in de politiepraktijk een logische stap voor de politiediensten.[8] Dit brengt ons tot de definitie van IGP. Deze luidt als volgt.

Definitie 3: IGP is de implementatie van het concept van intelligence in de context van de politiële bestrijding van criminaliteit.

In hoofdstuk vijf gaan wij dieper in op IGP en behandelen wij ook andere definities. Die definities leggen de nadruk op verschillende aspecten van IGP, zoals het sturen van het politiewerk (zie subsectie 5.4.2). Wij hebben er echter voor gekozen om ons met name op het kernbestanddeel van IGP te richten, te weten intelligence. IGP staat

[6] Het controleren en managen van risico's past binnen de risicosamenleving (Ericson en Haggerty 1997; Hudson 2003; Van der Woude 2010). Zie voor een inhoudelijke behandeling van de risicosamenleving subsectie 5.3.1.

[7] Overigens willen wij niet suggereren dat de politie in alle gevallen bewust intelligence kopieerde van de inlichtingen- en veiligheidsdiensten. Intelligence wordt bijvoorbeeld ook toegepast binnen het bedrijfsleven, waar het bekend staat als *business-intelligence*. Wij hebben geen direct bewijs waaruit blijkt dat het korps van Kent het concept van IGP van de inlichtingen- en veiligheidsdiensten heeft afgekeken. Het is echter wel een feit dat intelligence al sinds de Eerste Wereldoorlog (en wellicht daarvoor) het concept is volgens welke de inlichtingen- en veiligheidsdiensten werken (zie voor uiteenlopende bronnen over de geschiedenis van intelligence en verschillende inlichtingen- en veiligheidsdiensten: Deacon 1974; Knightly 1986; Keegan 2003; Thomas 2009).

[8] Zie Ratcliffe (2008). Ratcliffe is van mening dat de nadruk op intelligence vaak ten koste gaat van het element '*policing*' uit de definitie. Hij gaat hierbij echter voorbij aan het feit dat in het element intelligence de sleutel zit voor het begrijpen van IGP als concept. Het 'policing' is immers niets nieuws, intelligence lijkt daarentegen de innovatie te zijn. Zie ook: Gill en Phythian (2006).

immers voor *intelligence*gestuurde politie. Intelligence belooft (in theorie) de mogelijkheid van het geven van voorwaarschuwingen ten behoeve van veiligheidsvraagstukken. Dit maakt intelligence aantrekkelijk voor de moderne politie. Van de politie wordt namelijk steeds meer verwacht dat zij criminaliteit voorkomt (zie subsectie 5.2.5). Daartoe moet eerst een bepaald werkproces worden geïmplementeerd (de reeks van activiteiten betreffende informatieverzameling, analyse en verstrekken van informatie). Met intelligence wordt vervolgens het politiewerk gestuurd.

In het woord 'implementatie' ligt de focus van dit onderzoek. Het is namelijk één ding om een concept te kopiëren van de inlichtingen- en veiligheidsdiensten naar de politiepraktijk, de daadwerkelijke implementatie ervan is heel iets anders. Tussen de theorie van IGP en de praktijk zit dan ook een wereld van verschil. Een belangrijk doel van dit onderzoek is het verkrijgen van inzicht in de praktijk van IGP. Wij definiëren implementatie als volgt.

Definitie 4: Implementatie is het proces van (1) het operationaliseren van de abstracte elementen van IGP teneinde (2) IGP in gebruik te nemen in de politiepraktijk.

Hoewel het begrijpelijk is dat een concept als intelligence een bijzondere aantrekkingskracht heeft op de politie, is de implementatie ervan in de politiële context niet zonder problemen. Want hoe kan een concept als intelligence worden geoperationaliseerd en in de praktijk worden toegepast? Dit proces blijkt in de praktijk lastiger dan in theorie, mede omdat intelligence en andere gerelateerde elementen, zoals voorwaarschuwing en preventief beleid, door politiefunctionarissen verschillend kunnen worden geïnterpreteerd. Een bijkomend essentieel probleem is de scheiding tussen de veiligheidsdiensten en de politie. De bespreking van dit probleem brengt ons allereerst op de door ons gehanteerde terminologie met betrekking tot het werk van de inlichtingen- en veiligheidsdiensten.

Voor de lezer die niet bekend is met het inlichtingenjargon benoemen wij hieronder kort het verschil tussen (1) inlichtingendiensten en (2) veiligheidsdiensten (zie ook Abels en Willemse 2004: 84).

Definitie 5: Inlichtingendiensten zijn de offensieve diensten die zijn belast met de bescherming van de externe nationale veiligheid en die daarvoor informatie vergaren in en over het buitenland.

Definitie 6: Veiligheidsdiensten zijn de defensieve diensten die zijn belast met de bescherming van de binnenlandse nationale veiligheid .

Een inlichtingendienst beschermt de nationale veiligheid met name door het uitvoeren van inlichtingenoperaties in het buitenland, ook wel offensieve spionageactiviteiten genoemd. Een veiligheidsdienst beschermt de nationale veiligheid door middel van het uitvoeren van inlichtingenoperaties op het eigen grondgebied. Traditioneel was de Nederlandse Binnenlandse Veiligheidsdienst (BVD) belast met het beschermen van de nationale veiligheid en de Inlichtingendienst Buitenland (IDB) met de spionageactiviteiten in het buitenland. Inmiddels bestaat de IDB niet meer: de AIVD voert beide taken uit, en vandaar dat er gesproken wordt van een 'inlichtingen- en veiligheidsdienst' (zie De Graaf en Wiebes 1998; zie ook Abels en Willemse 2004: 84-87). Wanneer wij spreken van een veiligheidsdienst, doelen wij op de organisatie

die is belast met de bescherming van de interne nationale veiligheid. De term 'inlichtingen- en veiligheidsdienst' gebruiken wij voor het bredere inlichtingenwerk, dat naast de interne nationale veiligheid ook de offensieve spionage in het buitenland en de militaire inlichtingenfunctie omvat. Omdat wij ons richten op de interne nationale veiligheid, zullen wij in het vervolg met name de term 'veiligheidsdienst' hanteren.

Tot slot geven wij een definitie van de CIE.

Definitie 7: de Criminele Inlichtingeneenheden (CIE-en) zijn de afdelingen van de politie die zijn belast met de uitvoering van de CIE-taak, te weten (A) het runnen van informanten en/of (B) het verkrijgen van inzicht in de zware (georganiseerde) criminaliteit, terrorisme daarbij inbegrepen.

Uit deze definitie volgt dat ook afdelingen die binnen de politie formeel niet tot de organisatorische eenheid CIE worden gerekend, maar die wel zijn belast met het runnen van informanten of het verkrijgen van inzicht in de zware (georganiseerde) criminaliteit (zoals de Regionale Informatie Organisatie, RIO), door ons tot de CIE worden gerekend. Zie voor een nadere toelichting subsectie 4.4.3.

1.3 De scheiding van de veiligheidsdiensten en de politie

Na de Tweede Wereldoorlog zijn in delen van West-Europa veiligheidsdiensten en politiediensten van elkaar gescheiden. De gedachte is dat een veiligheidsdienst met verregaande executieve bevoegdheden, zoals de bevoegdheid om mensen te arresteren, kan uitgroeien tot een geheime politieke politie zoals de Gestapo of Stasi (zie Funder 2003; Rees 2007: 54). Deze diensten hebben een verregaand mandaat en treden vaak op naar eigen inzicht; van toetsing en controle door onafhankelijke (rechterlijke) instanties is nauwelijks sprake. Ze kennen geen grenzen aan de informatiebehoefte, hetgeen resulteert in een omvangrijke surveillance van de eigen bevolking. In veel democratische rechtsstaten bestaat de angst voor oncontroleerbare geheime politiediensten die zo diep ingrijpen op de persoonlijke levenssfeer van de burger dat er van privacy en andere grondrechten niet veel meer overblijft. Het is dan ook met name een principiële angst: het slechten van de barrières tussen de veiligheidsdiensten en de politie maakt een geheime politieke politie theoretisch gezien mogelijk. Om het ontstaan van zo'n geheime, politieke politie te voorkomen hebben veel westerse democratische rechtsstaten diverse organisatorische en juridische maatregelen getroffen, waarbij met name het inlichtingenwerk van de veiligheidsdienst werd gescheiden van het executieve optreden van de politie. Een veel gehoorde stelling is dan ook dat de scheiding tussen inlichtingenwerk en executief optreden sinds de Tweede Wereldoorlog werd gezien als een kenmerk en zelfs een garantie voor het bestaan van een democratische rechtsstaat (zie Fijnaut 2004: 15). Dit geldt echter niet voor alle democratische rechtsstaten. Met betrekking tot de scheiding tussen de politie en veiligheidsdiensten behandelen wij twee modellen: een 'Engels' en een 'Frans' model.

1.3.1 Het Engelse model

Het Engelse model brengt een strikte scheiding aan tussen veiligheidsdiensten en politiediensten met executieve (politie)bevoegdheden. Zo is de Engelse

veiligheidsdienst MI5 een veiligheidsdienst zonder executieve (politie) bevoegdheden. Dit model wordt ook in Nederland en Duitsland gehanteerd.

In het naoorlogse West-Duitsland was deze scheiding het duidelijkst. Om een nieuwe Gestapo te voorkomen, werd er een aparte veiligheidsdienst in het leven geroepen, het *Bundesambt für Verfassungsschutz*. Deze dienst werd gescheiden van de politiediensten en kreeg geen executieve bevoegdheden: de dienst richtte zich exclusief op het beschermen van de 'nationale veiligheid' (in de zin van de bescherming van de waarden van de Grondwet) en de werkzaamheden waren beperkt tot het verzamelen van informatie over mogelijke bedreigingen van die nationale veiligheid (zie Fijnaut 2004: 15; Van Daele en Vangeebergen 2006: 27-28). Het *Bundesambt für Verfassungsschutz* had dan ook geen bevoegdheden om bijvoorbeeld iemand te arresteren (Fijnaut 2004: 14-15). De Duitse scheiding van de diensten staat bekend als het *Trennungsgebot* en heeft een semiconstitutionele status (Van Daele en Vangeebergen 2006: 29).

1.3.2 Het Franse model

Het Franse model gaat uit van een wezenlijk andere organisatie. Er is daar geen sprake van een strikte organisatorische of functionele scheiding tussen de (inlichtingen- en) veiligheidsdiensten en de politie. De belangrijkste Franse veiligheidsdienst DCRI (*Direction Centrale du Renseignement Intérieur*, een combinatie van de vroegere *Direction centrale des renseignements généraux*, oftewel DCRG en de *Direction de la Surveillance du territoire*, oftewel DST) ressorteert onder de nationale politie (*Direction générale de la police nationale*) (Van Daele en Vangeebergen 2006: 62-63). Deze veiligheidsdienst heeft dus opsporingsbevoegdheid. Dit Franse model zien we ook terug bij de Deense veiligheidsdienst PET, de Zweedse SAPO, het Finse SUPO en de *Katsepolitsei* van Estland. Omdat Nederland het Engelse model heeft geïmplementeerd, gaan wij uit van dat model en laten wij het Franse model verder buiten beschouwing.

1.4 De Nederlandse scheiding tussen de AIVD en de politie

Ook in Nederland heeft de angst voor een geheime politieke politie, zoals de Gestapo, ertoe geleid dat de politiediensten grotendeels gescheiden werden van de Nederlandse inlichtingen- en veiligheidsdiensten, de Binnenlandse Veiligheidsdienst (BVD, nu AIVD), de Militaire Inlichtingendienst (MID, nu MIVD) en de al eerder genoemde IDB.[9] In de jaren '90 van de vorige eeuw kreeg de BVD een wettelijke basis: de Wet op de Inlichtingen- en Veiligheidsdiensten (WIV) regelde onder andere de taakstelling en de bevoegdheden die de BVD ter beschikking stonden. In deze wet is ook de scheiding tussen politiediensten en de BVD opgenomen: medewerkers van de dienst hebben geen bevoegdheid om strafbare feiten op te sporen (artikel 9 WIV 2002). Inmiddels is de dienst in 2002 van naam veranderd, en staat hij nu bekend als de 'Algemene Inlichtingen en Veiligheidsdienst', oftewel de 'AIVD'. Aan het

[9] Dit neemt niet weg dat zowel de politie als de AIVD vallen onder het ministerie van Binnenlandse Zaken. Voor de politie geldt dit voor zover het de beheerscomponent betreft. Als het gaat om de handhaving van de rechtsorde of de openbare orde zijn respectievelijk de officier van justitie) en de burgemeester van de grootste gemeente van het regiokorps het bevoegd gezag, zie artikelen 12 en 13 Politiewet 1993. Overigens ging er aan de scheiding een strijd vooraf tussen het ministerie van Binnenlandse Zaken en het ministerie van Justitie: de laatste was niet van plan om zomaar zijn eigen inlichtingenafdelingen op te doeken. Zie voor een behandeling van deze geschiedenis: Engelen (1995).

uitgangspunt dat de politie en de AIVD gescheiden dienen te zijn, is echter niets veranderd: artikel 9 van de Wet op de Inlichtingen en Veiligheidsdiensten 2002 (WIV 2002)[10] stelt nog steeds dat ambtenaren van de AIVD niet de bevoegdheid hebben om opsporingshandelingen te verrichten. Het neemt echter niet weg dat de organisaties zeer dicht bij elkaar liggen. Dit werd misschien nog wel het beste onder woorden gebracht door een medewerker van de AIVD tijdens één van onze interviews in het kader van dit onderzoek.

"*Politie en inlichtingendiensten zijn twee zijden van dezelfde medaille. Ze liggen heel dicht tegen elkaar aan, maar zullen elkaar nooit raken.*" Interview (voormalig) medewerker AIVD (A), januari 2008

Op zichzelf is het bovenstaande citaat een duidelijk uitgangspunt, maar is het nog wel houdbaar nu er sprake lijkt te zijn van een 'oorlog tegen het terrorisme'? Veel regeringen zijn in ieder geval van mening dat dit niet zo is en in deze landen (bijvoorbeeld de V.S.) wordt het belang van samenwerking tussen de inlichtingen- en veiligheidsdiensten en opsporingsdiensten boven de oude scheiding tussen de diensten geplaatst. De eerste verschuivingen vonden echter eerder plaats dan de aanslagen van 11 september 2001: zij waren volgens sommigen een directe reactie op het uiteenvallen van de Sovjet-Unie (zie Andreas en Nadelmann 2006: 157-165).

1.5 Vanaf 1990: veiligheidsdiensten op zoek naar een nieuwe markt

Met de val van de Sovjet-Unie viel ook de belangrijkste vijand van de westerse inlichtingen- en veiligheidsdiensten weg. Tijdens de Koude Oorlog was de vijand gemakkelijk te duiden: het was de Sovjet-Unie, en hiervan ging met name een militaire dreiging uit. Toen deze ophield te bestaan, zagen de westerse (inlichtingen- en) veiligheidsdiensten zich geconfronteerd met mogelijke bezuinigingen en inkrimping. In de woorden van Bob Gates, de directeur van de CIA in het begin van de jaren '90 (direct na de val van de Sovjet-Unie): "(het is een) *nieuwe wereld daarbuiten, aanpassen of sterven*" (Weiner 2007: 469). De diensten moesten aldus hun eigen bestaansrecht aantonen en op zoek naar 'nieuwe markten'. Al snel bleek dat de internationale georganiseerde criminaliteit hier bijzonder goed geschikt voor was. De Amerikaanse denktank *Center for Strategic and International Studies* organiseerde in 1994 een conferentie getiteld *Globalized Organized Crime: The New Evil Empire*. In een samenvatting van deze conferentie stelde deze denktank het volgende: "*The dimensions of global organized crime present a greater international security threat than anything Western democracies had to cope with during the cold war.*" (Andreas en Nadelmann 2006: 158). In deze periode richtte de inlichtingen- en veiligheidsdiensten zich daarom wereldwijd steeds meer op de georganiseerde criminaliteit. Georganiseerde criminaliteit lijkt in deze periode één van de nieuwe markten te zijn waaraan de inlichtingen- en veiligheidsdiensten hun bestaansrecht zouden kunnen ontlenen` (Andreas en Nadelmann 2006: 235-237). Dit gold ook voor de georganiseerde criminaliteit in Nederland. Vanaf het begin van jaren '90 van de vorige eeuw had de georganiseerde criminaliteit de aandacht van de BVD. Net als de Amerikaanse inlichtingen- en veiligheidsdiensten werd de BVD in deze periode geconfronteerd met het wegvallen van de dreiging van de Sovjet-Unie. Het is daarom

[10] Wet van 7 februari 2002 houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten, Stb. 2002, 148.

'redelijk logisch' te veronderstellen dat de BVD, evenals de andere Westerse veiligheidsdiensten, in de georganiseerde criminaliteit een nieuwe markt vond.[11]

Tegenover deze logische veronderstelling staat de mening van twee medewerkers van de dienst, Abels en Willemse. Zij geven aan dat de verandering in doelstelling bij de dienst al eerder plaatsvond, namelijk in het begin van de jaren '80 van de vorige eeuw. De veelgehoorde stelling dat er sprake was van een zoektocht van de dienst naar nieuwe vijanden bestempelen zij als een 'karikatuur' (Abels en Willemse 2004: 86-89). Fijnaut (2004: 36) geeft in dit opzicht aan dat voor West-Europa geldt dat er met betrekking tot de aandacht van inlichtingen- en veiligheidsdiensten voor de georganiseerde criminaliteit wellicht beter gesproken kan worden van een parallelle ontwikkeling dan van een oorzaak/gevolgontwikkeling. De val van de muur en het communisme staat los van de toegenomen aandacht voor de georganiseerde criminaliteit: sinds het einde van de jaren '80 wordt georganiseerde criminaliteit gezien als een belangrijk maatschappelijk vraagstuk dat vraagt om een krachtig tegen-beleid (Fijnaut 2004: 36).

Hoe dan ook, in de jaren '90 werd door de BVD voor het eerst (kenbaar) aandacht besteed aan het fenomeen van de georganiseerde criminaliteit. Zo werd in het jaarverslag van 1994 kort melding gemaakt van de aanwezigheid van de Russische maffia op Nederlands grondgebied (van Traa 1996). Andere zaken die gedurende de jaren '90 door de dienst werden onderzocht waren onder meer (1) XTC-handel, (2) mogelijke corruptie als onderdeel van de georganiseerde criminaliteit en (3) betrokkenheid van bepaalde etnische minderheden bij deze nieuwe vorm van zware criminaliteit.[12] De BVD leek zich hiermee op een terrein te begeven dat voorheen exclusief was voorbehouden aan de politie. Dit betekende dat de politie en de BVD elkaar in toenemende mate zouden tegenkomen. Deze ontluikende ontwikkeling kreeg een verdere stimulans door de aanslagen van 11 september 2001.

1.6 Vanaf 2000: terrorisme als nieuwe markt voor de politie

De bestrijding van terrorisme heeft van het begin af aan tot het takenpakket van veiligheidsdiensten behoord. De BVD waarschuwde reeds vroeg in de jaren '90 van de vorige eeuw als een van de eersten voor het gevaar van islamitisch terrorisme, en heeft dit al die tijd als een aandachtsgebied beschouwd (Abels 2007: 125-136). Vanaf de aanslagen van 11 september 2001 begaf de politie zich echter ook steeds meer op dit terrein.[13] In eerste instantie ontbrak het politie en justitie op dat moment aan

[11] Dat het fenomeen van de georganiseerde criminaliteit op zichzelf voldoende aanleiding geeft voor de aandacht van inlichtingen- en veiligheidsdiensten (vanwege de nauwe relatie tussen georganiseerde criminaliteit en terrorisme enerzijds en de belangen die de georganiseerde criminaliteit in het gedrang brengt anderzijds), doet onzes inziens niets af aan de constatering dat het aan het begin van de jaren '90 een nieuwe markt voor de inlichtingen- en veiligheidsdiensten was (zie Fijnaut 2004: 36).

[12] Jaarverslagen BVD 1996, 1997,1998, te downloaden van www.aivd.nl, gezien op 20 december 2009.

[13] Voor een gedetailleerde beschrijving van de periode van na de Koude Oorlog verwijzen wij naar Andreas en Nadelmann (2006: 157-165). Deze auteurs richten zich met name op de toenemende activiteiten van de Amerikaanse inlichtingengemeenschap op terreinen die traditioneel toebehoren aan de opsporingsdiensten en zij citeren onder meer Stewart Barker, het voormalige hoofd van de grootste Amerikaanse veiligheidsdienst, de *National Security Agency* (NSA): *"(...) as topics like international narcotics trafficking, terrorism, alien smuggling, and Russian organized crime rose in priority for the intelligence community, it became harder to distinguish between targets of law enforcement and those of national security*" (2006: 160). Zoals gezegd richten deze auteurs zich met name op de ontwikkeling van het opnemen van criminaliteit in de doelstelling van de inlichtingen- en veiligheidsdiensten. Zij behandelen de tegenhanger (de opsporingsdiensten die zich op het terrein van de inlichtingen- en veiligheidsdiensten begeven) bijna niet. Bij de door Andreas en Nadelmann beschreven ontwikkeling

relevante kennis, ze hadden hier namelijk jarenlang weinig tot geen aandacht aan besteed. Voor hen was terrorisme dus een nieuwe markt. Hieronder behandelen we achtereenvolgens het primaat van de terrorismebestrijding (subsectie 1.6.1), veranderingen met betrekking tot terrorismebestrijding (subsectie 1.6.2) en gevolgen voor de verhouding (subsectie 1.6.3).

1.6.1 Het primaat van de terrorismebestrijding

Het primaat van de terrorismebestrijding lag gedurende de jaren '90 van de vorige eeuw met name bij de BVD, met als gevolg dat de voor terrorismebestrijding relevante kennis en expertise daar werd opgedaan. Maar het werd na de aanslagen van 11 september al snel duidelijk dat de BVD/AIVD niet lang meer de enige partij zou zijn die betrokken zou worden bij het bestrijden van terrorisme: "*een enorme proliferatie van het aantal actoren op (het contra-terrorisme) gebied was het gevolg, compleet met de even logische als onvermijdelijke afstemmings- en competentievraagstukken*" (Abels 2007: 126). Eén van deze actoren is de politie. De AIVD had echter zoals gezegd een inhoudelijke voorsprong op de politie, en zij kreeg mede daarom een bepalende rol bij de aanpak van het islamitisch terrorisme.

De traditionele doelstelling van de AIVD, te weten het tijdig signaleren en voorkomen van bedreigingen van de nationale veiligheid, sluit goed aan bij de specifieke behoeften met betrekking tot terrorismebestrijding. Het nieuwe islamitische terrorisme wordt namelijk door sommigen ook wel 'catastrofaal terrorisme' genoemd vanwege de doelstelling om zoveel mogelijk burgerslachtoffers te maken (Rosenthal et al. 2006; Duyvesteyn en de Graaf 2007).[14] Aanslagen dienen daarom met name te worden voorkomen; de bestrijding dient proactief en preventief te zijn. Hiervoor heeft een inlichtingendienst zoals de AIVD verregaande bevoegdheden. Zo mag de dienst telefoontaps inzetten, agenten en informanten runnen,[15] stelselmatig individuen observeren en dergelijke. Over het algemeen zijn dit bevoegdheden die de politie ook heeft, maar de AIVD mag deze bevoegdheden traditioneel in een eerder stadium inzetten dan de politie. Er behoeft geen sprake te zijn van een concrete verdenking van een specifiek strafbaar feit, hetgeen voor de klassieke politie lange tijd wel het criterium voor de toepassing van opsporingsbevoegdheden is geweest.[16] In bepaalde

---

kunnen echter ook kanttekeningen worden geplaatst. Fijnaut (2004) stelt bijvoorbeeld dat de FBI ver voor de val van de Sovjet-Unie betrokken was bij de strijd tegen georganiseerde criminaliteit. De FBI is een bijzondere organisatie in de zin dat zij zowel de functie van veiligheidsdienst als die van opsporingsdienst heeft (vergelijkbaar met het hierboven benoemde Franse model). Omdat wij ons in dit onderzoek met name op de Nederlandse situatie richten, zullen wij de Amerikaanse diensten verder buiten beschouwing laten.

[14] Interessant is dat in dit boek ook een bijdrage staat van een medewerker van de AIVD. Deze persoon geeft aan dat "*termen als catastrofaal en apocalyptisch terrorisme worden gelanceerd om aan te geven hoe nieuw en uitzonderlijk de dreiging van het islamitisch of jihadistisch terrorisme is. De vraag is echter of deze voorstelling van zaken wel correct is.*" Hij trekt ("*for the sake of argument*") historische parallellen tussen de West-Europese geschiedenis en het jihadistisch terrorisme. Zie Duyvesteyn en de Graaf (2007: 129-130) Het gebruik van termen als 'catastrofaal terrorisme' blijft aldus niet zonder kritiek, kennelijk ook niet bij de medewerkers van de AIVD.

[15] Een agent is de feitelijke spion. Hij wordt door de AIVD aangestuurd en verzamelt gericht informatie. Een informant is iemand die incidenteel over informatie beschikt en deze doorspeelt aan de AIVD, zonder dat er vanuit de kant van de AIVD sprake is van sturing. Zie ook subsectie 3.3.6.

[16] Hier kwam op 01-02-2000 met de inwerkingtreding van de Wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen, beter bekend als de Wet Bijzondere Opsporingsbevoegdheden (Wet BOB), verandering in (Wet van 27 mei 1999, Stb. 245). Naast de concrete verdenking van artikel 27 WvSv kreeg de politie de mogelijkheid om bij een redelijk vermoeden dat in een bepaald

gevallen gaan de bevoegdheden van de AIVD (iets) verder dan die van de politie. Zo kan de dienst een agent bepaalde strafbare feiten laten plegen indien dit van belang is voor het uitvoeren van zijn taak.[17] Informanten van de politie mogen dit in de regel niet (zie sectie 4.3 voor een inhoudelijke behandeling van de figuur van de politie-informant). De politie is traditioneel reactief en is beperkt in de bevoegdheden die zij kan toepassen. Op het eerste gezicht lijkt er dus sprake te zijn van een duidelijke afbakening van de taken en bevoegdheden van de AIVD en de politie op het gebied van de terrorismebestrijding. De genoemde afbakening alsmede de veronderstelde invulling van de taken leidt tot drie duidelijke verschillen tussen de AIVD en de politie: (1) de AIVD heeft een kennisvoorsprong op de politie en is daarmee leidend in de aanpak van terrorisme, (2) de AIVD is proactief en preventief, de 'klassieke' politie is reactief en (3), de AIVD heeft meerdere en verdergaande bevoegdheden, hetgeen onder meer het gevolg is van het proactieve van de AIVD (proactiviteit impliceert immers in een vroeg stadium informatie verzamelen). Op al deze drie vlakken vinden belangrijke veranderingen plaats.

1.6.2 Drie veranderingen bij de terrorismebestrijding

Hieronder beschrijven wij de veranderingen op de drie genoemde vlakken. Allereerst is er het verschil in kennis tussen de AIVD en de politie. De kennisachterstand van de politie wordt steeds kleiner naarmate de politie zich langer op terrorismebestrijding richt. De speciale eenheden belast met terrorismebestrijding ontwikkelen specialistische kennis. Daartoe nemen ze experts in dienst: arabisten, antropologen en islamologen worden gebruikt vanwege hun gedetailleerde kennis omtrent diverse aspecten van islamitisch terrorisme. In tegenstelling tot 2001 draagt de politie van 2011 ook kennis van de islam, de rol van radicalisering bij terrorisme en andere relevante contextuele en detaillistische aspecten van het fenomeen. Deze ontwikkeling moet echter niet worden overschat. Daar waar de AIVD met name hoger opgeleide medewerkers in dienst heeft, bestaat de politie nog steeds voor het grootste gedeelte uit lager opgeleide medewerkers. In dat opzicht zal de AIVD altijd wel een kennisvoorsprong behouden. Daar staat tegenover dat de politieorganisatie veel groter is en dus in staat is (of zou moeten zijn) om meer capaciteit vrij te maken voor terrorismebestrijding en kennisontwikkeling op dat gebied. Hoe groot deze verandering is, kunnen wij echter niet vaststellen. Wij hebben geen zicht op alle verschillende kennisprojecten die binnen de politie en de AIVD plaatsvinden.

Op het tweede vlak is sprake van toenemende proactiviteit van de politie. Dit volgt onder meer uit de ontwikkeling en implementatie van IGP. Maar ook de nieuwe rol bij de bestrijding van terrorisme leidt tot een verdergaande proactivering. In het kader van de terrorismebestrijding wordt van de politie verwacht dat zij een bijdrage levert aan het voorkomen van terroristische aanslagen. Hiervoor is de zelfstandige opbouw en instandhouding van een goede informatiepositie onontbeerlijk. Daar waar eerder de zelfstandige opbouw van een informatiepositie ondergeschikt was aan de opsporingstaak, is dit inmiddels verworden tot een zelfstandige doelstelling van de

---

georganiseerd verband misdrijven worden beraamd of gepleegd tegen dat georganiseerde verband een opsporingsonderzoek op te starten (artikel 126o WvSv). Deze wetswijziging ziet op de opsporing van georganiseerde criminaliteit. Een redelijk vernoeden dat bepaalde strafbare feiten daadwerkelijk zijn begaan (en wie binnen dat georganiseerde verband verantwoordelijk is voor welk concrete strafbare feit) is bij de opsporing van georganiseerde criminaliteit dus niet noodzakelijk.

[17] Waar wij gebruik maken van 'hij' en 'zijn' kan ook 'zij' en 'haar' worden gelezen. Omwille van de leesbaarheid kiezen wij voor het gebruiken van 'hij' en 'zijn'.

politie (zie Koelewijn 2009; Kielman 2010). Deze beweging dateert overigens al van voor 11 september 2001, maar het politieke en maatschappelijke klimaat van na de aanslagen is de belangrijkste katalysator achter deze ontwikkeling.

Op het derde vlak kreeg de politie onder andere ingrijpende opsporingsbevoegdheden die zij kon inzetten tegen mensen die (nog) niet verdacht werden van strafbare feiten. Naast de verruiming van de mogelijkheid tot het verzamelen van informatie over verdachte personen, werden ook de mogelijkheden verruimd om gegevens omtrent niet verdachte personen te verwerken. De politie lijkt dus de bevoegdheden, doelstellingen en werkwijze van een veiligheidsdienst voor een deel te hebben overgenomen. Dit stimuleert de ontwikkeling en implementatie van IGP alleen maar verder. Immers, voor het voorkomen van aanslagen is een goede informatiepositie onontbeerlijk. Deze informatie moet worden geanalyseerd en de geanalyseerde informatie (vaak intelligence genoemd), dient aan de basis van de politiële besluitvorming te liggen. Dit zijn allemaal ingrediënten van IGP.

1.6.3 Gevolgen voor de verhouding

De belangen die zijn gemoeid met de bestrijding van terrorisme en de hieruit voortvloeiende ontwikkelingen, zoals de proactivering van de politie, hebben grote gevolgen voor de verhouding tussen de politie en de AIVD in de praktijk. Met de term 'verhouding' bedoelen we de betrekking tussen de twee diensten in de bredere zin van het woord. Hieronder vallen samenwerking, uitwisseling van informatie, maar bijvoorbeeld ook concurrentie. Wij maken een onderscheid tussen de formeel juridische verhouding, de organisatorische verhouding en de informele verhouding in de praktijk. Wij spraken eerder (in sectie 1.3) over de scheiding tussen de diensten. Deze scheiding is de formeel juridische verhouding tussen de diensten. Met andere woorden: het is de hoofdregel voor de verhouding tussen de diensten. Maar de verhouding is breder dan de scheiding. Ondanks het feit dat de diensten van elkaar gescheiden zijn, zullen zij in bepaalde gevallen toch moeten samenwerken. Zo is het in het kader van de terrorismebestrijding niet langer geoorloofd om geen informatie met elkaar te delen. Het is namelijk goed voorstelbaar dat de informatie waarover de ene dienst beschikt nou net dat ene ontbrekende stukje van de puzzel van de andere dienst is. Het niet delen van deze puzzelstukjes leidt mogelijk tot het niet kunnen voorkomen van aanslagen.[18] Het delen van informatie is echter voor de AIVD geenszins vanzelfsprekend. Het is immers niet voor niets een geheime dienst, en een geheime dienst zal vanwege de mogelijke schade aan de eigen effectiviteit en het gevaar voor zijn bronnen zelden informatie aan derden verstrekken. Voorts is de politie evenmin geneigd om informatie te delen (Kop en Klerks 2009: 48-51; Calster en Vis 2009). Hier spelen, net als bij de veiligheidsdiensten, zaken als afscherming van methoden, technieken en bronnen, maar ook concurrentieoverwegingen een rol. Kennis is namelijk macht.[19] Het niet delen van informatie draagt als extra gevaar in zich dat beide diensten elkaar in de wielen gaan rijden. Immers, als de politie informatie heeft over een terroristisch netwerk waar ook de AIVD een agent in heeft, maar de politie is niet van het bestaan van de agent op de hoogte, dan kan het zomaar

[18] Adviescommissie Informatiestromen Veiligheid, *Data voor Daadkracht, Gegevensbestanden voor veiligheid: observaties en analyse*, 2006, pp. 17-18. Te downloaden van: http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2007/08/30/rapport-data-voor-daadkracht/datavoordaadkracht.pdf, gezien op 13 juli 2010.

[19] In sectie 2.3 zullen we de verschillende benaderingen en de daaruit voortvloeiende redenen voor geheimhouding behandelen.

gebeuren dat de betreffende agent wordt aangehouden en de AIVD zijn informatiepositie kwijt is. Dit behoeft nog geen ramp te zijn indien de politie de hele organisatie oprolt, maar wat nu als die bron van de AIVD nou net in de buurt was van een andere terroristische cel die niet bij de politie bekend was? Dit laatste kan grote gevolgen hebben voor de effectiviteit van de terrorismebestrijding. Al met al kunnen de AIVD en de politie het zich niet meer veroorloven om geen informatie met elkaar te delen.

Terrorisme is derhalve een nieuwe markt voor de politie, en dit leidt ertoe dat de AIVD en de politie in dezelfde vijver vissen en wellicht steeds verder naar elkaar toe groeien. Deze ontwikkeling is niet zonder kritiek gebleven, hetgeen het onderwerp is van de volgende sectie.

1.7 Kritiek op een mogelijke vermenging van de AIVD en de politie

De hierboven beschreven ontwikkelingen zetten de eerder genoemde scheiding tussen de diensten aanzienlijk onder druk. Deze scheiding behoort, zoals eerder gezegd, eigenlijk tot één van de kenmerken van de democratische rechtsstaat. Het is dan ook weinig verwonderlijk dat de ontwikkelingen die in sectie 1.6 aan de orde zijn gesteld niet zonder kritiek zijn gebleven.

Op 22 december 2004 adviseerde het College Bescherming Persoonsgegevens (CBP) de minister van Justitie in het kader van het conceptwetsvoorstel bijzondere bevoegdheden tot opsporing van terroristische misdrijven. Het CBP waarschuwde specifiek voor een toenemende vermenging van de taken van de inlichtingen- en veiligheidsdiensten en de politie.[20] Eén van de waarborgen voor een adequate gegevensbescherming vormt de taakscheiding van deze diensten, aldus het CBP. De AIVD mag traditioneel meer dan de politie en mag dat in een eerder stadium omdat het belang van de staatsveiligheid groter is dan het belang van criminaliteitsbestrijding. De diensten waren in 2004 nog strikt van elkaar gescheiden, zowel juridisch als organisatorisch, maar volgens het CBP veranderde dit in toenemende mate.

Inmiddels (2011) lijkt het CBP de waarschuwing voor een vermenging over een enigszins andere boeg te gooien. De ontwikkeling is als volgt. In het jaarverslag van 2009 waarschuwt het CBP voor het verschijnsel dat de inlichtingen- en veiligheidsdiensten steeds meer zelfstandig toegang tot de gegevens van de politie krijgt, hetgeen betekent dat de laatste de controle over de gegevens verliest. Dit brengt het gevaar met zich mee dat de context van de gegevens voor de inlichtingendienst verloren gaat. Het gevolg hiervan kan zijn dat analyses tekortschieten en dat er verkeerde operationele beslissingen worden genomen.[21] Het CBP ontwaart hier dan ook een zeker operationeel risico.

De bovenstaande kritiek komt niet alleen van de zogenoemde 'privacy-waakhonden'; ook in de internationale academische literatuur wordt er vaak gewaarschuwd voor een dergelijke vermenging (zie Gill en Phythian 2006; Brodeur 2007). Maar net als bij de vraag naar de praktijk van IGP is hier de vraag gerechtvaardigd in hoeverre de gevreesde vermenging in de praktijk daadwerkelijk plaatsvindt: groeien de diensten naar elkaar toe en werken ze meer samen? Een relevante vraag hierbij is: is er sprake van een voor de samenwerking noodzakelijk vertrouwen tussen de diensten? Een bijzonder spanningselement is dat de relatie

[20] Te downloaden van: http://www.cbpweb.nl, gezien op 21 januari 2009.

[21] College Bescherming Persoonsgegevens, Jaarverslag 2009, pagina 32. Te downloaden van: http://www.cbpweb.nl/downloads_jaarverslagen/Jaarverslag_2009.pdf, gezien op 27 april 2010.

traditioneel wordt gekenmerkt door een verregaande mate van geheimhouding. Wanneer er tussen twee partijen sprake is van geheimhouding over en weer, wordt een vertrouwensrelatie steeds moeilijker (zie sectie 8.3). Dit onderstreept de complexiteit van de verhouding. We herhalen daarom nogmaals het onderwerp van dit onderzoek: (1) de vraag naar de mate van implementatie van IGP in de CIE-praktijk en (2) de invloed hiervan op de scheiding tussen de AIVD en de CIE. In de volgende sectie behandelen wij de probleemstelling en onderzoeksvragen die meer inzicht dienen te geven in dit onderwerp.

1.8 Probleemstelling en onderzoeksvragen

De opkomst van georganiseerde criminaliteit in West-Europa in de jaren '80 en '90 van de vorige eeuw en de terroristische aanslagen aan het begin van de 21e eeuw hebben ertoe geleid dat er aan de Nederlandse politie nieuwe eisen worden gesteld. De politie moet steeds eerder en op eigen initiatief optreden en ingrijpen om zo mogelijke zware criminaliteit en terrorisme te voorkomen; met andere woorden: de Nederlandse politie moet proactiever worden. Hiertoe krijgt zij nieuwe bevoegdheden die haar in staat stellen om in een steeds eerder stadium informatie te verzamelen omtrent criminaliteit en terrorisme. Naast nieuwe (juridische) bevoegdheden zal de politie ook haar eigen werkprocessen en werkmethoden moeten herstructureren en aanpassen om proactiever te kunnen worden. IGP beoogt dit te doen.

IGP kan worden gezien als een nieuw politieparadigma. Het is als het ware de noodzakelijke herijking van het politiebestel. IGP vormt de politie om van een traditionele, reactieve politiedienst naar een modernere proactieve variant (zie Ratcliffe 2008). De politie krijgt hierdoor steeds meer kenmerken die met de kenmerken van de veiligheidsdiensten vergelijkbaar zijn. Sommige auteurs concluderen dan ook dat de politie steeds verder ontwikkelt van een klassieke reactieve politie naar een met veiligheidsdiensten vergelijkbare proactieve organisatie (Gill en Phythian 2006; Brodeur 2007). Inderdaad brengen de in deze context genoemde publicaties ons tot de volgende vier observaties betreffende de veiligheidsdiensten en de politie: (1) ze hebben vergelijkbare bevoegdheden, (2) ze kunnen deze in dezelfde fase toepassen, (3) ze richten zich op dezelfde fenomenen en (4) ze werken ook volgens dezelfde methode. Derhalve rijst de vraag waarin deze organisaties nog van elkaar verschillen. Dit brengt ons tot de volgende probleemstelling (PS).

PS: Wat zijn de gevolgen van de implementatie van het concept van intelligence in de context van de Nederlandse opsporing voor de verhouding tussen de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Criminele Inlichtingeneenheid (CIE) van de Nederlandse politie bij de bestrijding van georganiseerde criminaliteit en terrorisme?

De bovenstaande probleemstelling leidt tot vier onderzoeksvragen. De eerste twee onderzoeksvragen zien op de conceptuele verhouding tussen de veiligheidsdiensten en de politie en het concept IGP. Deze vragen luiden als volgt.

OV 1: Wat zijn de traditionele kenmerken van veiligheidsdiensten en de politie?

OV 2: Wat is het concept IGP en hoe beoogt dit concept de traditionele Nederlandse CIE te veranderen?

In de opsporing- en inlichtingenwereld wordt het predicaat 'intelligence' op veel verschillende verschijnselen toegepast. Met name bij de politie worden er verschillende eigenschappen en mogelijkheden toegeschreven aan intelligence. Wij hebben gekozen voor de definitie van Gill en Phythian (definitie 1, sectie 1.2). Wij beantwoorden in hoofdstuk twee OV 1 aan de hand van het concept van intelligence zoals het vorm heeft gekregen binnen de veiligheidsdiensten. In hoofdstuk drie en vier behandelen wij respectievelijk de AIVD en de traditionele CIE. Daarna behandelen wij in hoofdstuk vijf de wijze waarop de politie vorm geeft aan IGP.

De derde onderzoeksvraag gaat dieper in op de praktijk van IGP en luidt als volgt.

OV 3: In hoeverre is IGP geïmplementeerd in de Nederlandse CIE-praktijk?

De context van de veiligheidsdiensten is een hele andere dan die van de CIE. Binnen de specifieke context van de veiligheidsdiensten is het concept van intelligence gedurende een lange periode ontwikkeld. Vanwege de interactie tussen de context en de veiligheidsdienst heeft intelligence haar specifieke kenmerken en kwaliteiten gekregen (zie de definitie van intelligence in sectie 1.2). Overigens is deze interactie erg complex: actor en context (of *agency* en *structure*) beïnvloeden elkaar en dit leidt tot specifieke kenmerken van zowel actor als context. Omdat de context van de politie een andere is dan die van de veiligheidsdiensten en de organisaties derhalve ook verschillen, zal de interactie tussen actor en context heel verschillend van aard zijn in vergelijking met de veiligheidsdiensten. Volgens sommigen is de term IGP, in de zin van 'intelligent opsporen', dan ook innerlijk tegenstrijdig, zoiets als 'militaire muziek' (zie Gill 2000: xi). De politie zou volgens deze critici vanwege uiteenlopende redenen niet in staat zijn om intelligent op te sporen. De politieorganisatie wordt namelijk (onder meer) gekenmerkt door een zeer sterk ontwikkeld 'waan van de dag denken', en dit verhoudt zich slecht tot de meer analytische benadering van criminaliteit zoals IGP (zie Van der Vijver en Terpstra 2007: 372-374). Eigenlijk vereist intelligence een academische benadering waarvoor 'denkers' nodig zijn, terwijl de politieorganisatie pragmatisch is ingesteld en van oudsher met name 'doeners' in de gelederen heeft. Hiernaast kent de Nederlandse politie een notoir slechte ICT-organisatie die het werken met grote hoeveelheden data niet faciliteert en in sommige opzichten zelfs bemoeilijkt.[22] Voor een concept als IGP, dat onder meer draait op de analyse van data en informatie, is dit problematisch. Deze kenmerken van de politie bieden niet echt een voedzame bodem voor het succesvol implementeren van IGP. Hierbij komt ook nog dat de politieorganisatie van oudsher zeer moeilijk te reorganiseren valt vanwege een aanzienlijke weerstand

[22] De Algemene Rekenkamer heeft in 2003 onderzoek gedaan naar de ICT-situatie bij de politie. Toen bleken er grote tekortkomingen in de informatiehuishouding van de politie. Zie: Tweede Kamer, vergaderjaar 2003-2004, 28 350, nr 1 en 2. In 2005 werd er opnieuw door de Algemene Rekenkamer gekeken naar de politiële informatiehuishouding, en ook toen werd geconstateerd dat er nog steeds sprake was van tekortkomingen en werden er vraagtekens gezet bij de door de politie aangekondigde oplossingen. Zie: Algemene Rekenkamer, *Terugblik 2005*, te downloaden van: www.algemenerekenkamer.nl, gezien op 11 juni 2010. In 2010 beklaagde hoofdcommissaris Aalbersberg zich over de ICT-situatie bij de politie. De problemen zouden volgens hem 'catastrofale vormen hebben aangenomen' en 'de slagader' van zijn organisatie raken. Zie: www.novatv..nl, uitzending van 27 januari 2010. In juni 2011 heeft de Algemene Rekenkamer een rapport gepubliceerd waarin zij zich wederom zeer kritisch heeft uitgelaten over de ICT-situatie bij de Nederlandse politie. Zie: Algemene Rekenkamer (2011).

vanuit de eigen organisatie.[23] Het is dan ook nog maar de vraag of de politie daadwerkelijk in staat is om zich om te vormen van de traditionele, reactieve organisatie naar een proactieve, intelligencegestuurde organisatie.

Onze vierde onderzoeksvraag luidt als volgt.

OV 4: Wat is de verhouding tussen de AIVD en de CIE in de praktijk?

Binnen de politie bestaat het beeld dat IGP een belangrijke herijking van het politiewerk betekent. De mate waarin IGP het doel, de functie en de werkzaamheden van de politie verandert, heeft echter gevolgen voor de verhouding tussen het politiële inlichtingenwerk en dat van de veiligheidsdiensten.

Bij het beantwoorden van OV 4 behandelen wij ook de normatieve aspecten van de scheiding. Het kopiëren en toepassen van intelligence in de context van het politiewerk gebeurt namelijk niet zonder kritiek. Zo stelt een hoge Canadese politieleidinggevende: "*Intelligence led policing reeks of secret service, spy agency work- the capital 'I' in 'Intelligence*".[24] Anderen vullen deze kritiek aan en stellen omtrent de ontwikkeling naar IGP: "*the winds of history are blowing (...) towards authoritarianism*" (Sheptycki 2005). Is IGP de *Big Brother* waar al zo lang voor wordt gewaarschuwd?[25] Vooralsnog lijken dergelijke uitspraken niet te worden bevestigd of ontkracht door empirisch onderzoek, eenvoudigweg omdat dergelijk onderzoek nog niet is gedaan. Dit is vreemd, gezien de rechtsstatelijke implicaties van dergelijke ontwikkelingen; niet voor niets worden termen als '*big brother*', '*spy work*' en '*authoritarianism*' gebruikt. Bij het beantwoorden van OV 4 gaan wij ook in op deze normatieve aspecten van IGP: de scheiding tussen de inlichtingendienst en de politie staat mogelijk onder druk van IGP, maar wat is de waarde van die scheiding (zie subsectie 9.6.2)?

1.9 Onderzoekskeuze voor de term 'bestrijding'

In de probleemstelling geven wij aan dat wij ons richten op de *bestrijding* van georganiseerde criminaliteit en terrorisme. In plaats van 'bestrijden' zouden we ook andere gerelateerde termen kunnen gebruiken, zoals 'opsporen'. Opsporing is in belangrijke mate echter een juridische term en heeft een specifieke (juridische) betekenis voor de politie: in Nederland wordt het gedefinieerd als "*het onderzoek in verband met strafbare feiten onder gezag van de officier van justitie met als doel het nemen van strafvorderlijke beslissingen*", aldus artikel 132a WvSv. Dat deze definitie problematisch is voor het onderhavige onderzoek, volgt allereerst uit het feit dat de

[23] Dit heeft te maken met hardnekkige cultuurfenomenen en interne sociale organisatie. De politie is een *street-level bureaucracy*, wat er kortgezegd op neerkomt dat de man op de straat heel veel discretionaire ruimte heeft waarbinnen hij zelf kan bepalen wat hij doet (zie Lipsky 1980). Leidinggevenden kunnen hier moeilijk op sturen. Pogingen binnen de organisatie om hier wat aan te doen, leiden vaak tot kritiek en zelfs verzet binnen de gelederen van de '*ground level'* medewerkers. Zie voor de verschillende culturen en de interne sociale organisatie: Reuss-Ianni en Ianni (1983) en Van Calster, Roosma en Vis (2010); Zie voor een summiere weergave van veranderingen in de politiecultuur: Van der Torre (2007).

[24] Ex-RCMP Commissioner Zaccardelli in een publieke toespraak in 2005, geciteerd uit: Brodeur (2007: 29).

[25] In 2006 komen Tilburgse onderzoekers tot de conclusie dat de politie inmiddels zoveel bevoegdheden heeft dat *Big Brother*, een alwetende en alziende overheid, een realiteit kan worden. Maar zij signaleren ook dat het nog niet zo ver is. Zie Vedder et al. (2006).

AIVD geen onderzoek verricht met het oog op het nemen van een strafvorderlijke beslissing. Sterker nog: het is de AIVD expliciet verboden om aan opsporing in strafvorderlijke zin te doen (zie artikel 9 WIV 2002). Dit is de scheiding tussen de AIVD en de politie (CIE) waar ons onderzoek zich op richt.

Ook bezien vanuit het perspectief van de politieorganisatie is het gebruik van de term 'opsporing' binnen ons onderzoek minder voor de hand liggend dan het mogelijk op het eerste gezicht lijkt. De materiële waarheidsvinding vormt de kern van het gehele strafproces, en de opsporing is daar een belangrijk onderdeel van, maar het is zeker niet het enige onderdeel. Naast de opsporing richt de politie zich in toenemende mate op andere strategieën en wijzen van werken, zoals het tegenhouden van criminaliteit.[26] In de nieuwe visie van de politie op haar taak wordt tegenwoordig ook gesproken over de bestrijding van de georganiseerde criminaliteit en terrorisme als alternatief voor de opsporing. Dit kan een andere taakopvatting van de politie inhouden, waarbij de traditionele benadering van de opsporing (in de zin van waarheidsvinding) wordt losgelaten en andere benaderingen worden gekozen.

Opsporing in de zin van waarheidsvinding is binnen IGP nog steeds van groot belang, maar het is niet meer de enige benadering van het criminaliteitsprobleem. In haar lectorale rede formuleerde Mariëlle den Hengst-Bruggeling (2010: 15) het als volgt: "(...) *de nadruk (van intelligence) ligt niet op waarheidsvinding, maar vermindering van onzekerheid voor beslissers.*" Omdat met IGP de waarheidsvinding die in het kader van de opsporing plaatsvindt (deels) wordt losgelaten, hanteren wij de meer omvattende term van 'bestrijden'.

1.10 De onderzoekskeuze voor de CIE, georganiseerde criminaliteit en terrorisme

IGP is sinds haar ontstaan in het begin van de jaren '90 van de vorige eeuw uitgegroeid tot een concept dat al het politiewerk omvat. Wij richten ons echter op IGP bij de CIE. De CIE is specifiek belast met het verzamelen van informatie over georganiseerde criminaliteit en terrorisme door middel van het runnen van informanten. Daarnaast heeft de CIE ook als taak de analyse van politiële informatie teneinde inzicht te krijgen in de georganiseerde criminaliteit en terrorisme (zie artikel 10 lid 1 sub a Wpolg jo. artikel 4 CIE-regeling; zie ook hoofdstuk vier). Vanaf het begin van het onderzoek hebben wij het afgebakend tot de bestrijding van georganiseerde criminaliteit en terrorisme, en, gezien de taakstelling van de CIE, was de keuze om ons onderzoek daar te verrichten een logische keuze. Deze keuze voor een afbakening tot de bestrijding van georganiseerde criminaliteit en terrorisme verdient een nadere uitleg.

Aan de ene kant zullen wij de keuze moeten verantwoorden voor de focus op de CIE, en daarmee de bestrijding van georganiseerde criminaliteit en terrorisme, in plaats van overige politieonderdelen en de daarbij behorende taken, zoals eenheden die zijn belast met de aanpak van veelvoorkomende criminaliteit of overlast. Aan de andere kant verdient het uitleg waarom wij de bestrijding van zowel georganiseerde criminaliteit als terrorisme onderzoeken in plaats van ons toe te leggen op één van beide fenomenen. Wij geven drie redenen, te weten (A) IGP is oorspronkelijk bedoeld voor de bestrijding van georganiseerde criminaliteit, (B) georganiseerde criminaliteit

[26] 'Tegenhouden' wordt vaak voorgesteld als een nieuw concept voor de politie, maar het komt er feitelijk op neer dat de politie bijdraagt aan de preventie van criminaliteit. Preventie is al een oude taak van de politie. Voorbeelden van tegenhouden zijn bestuurlijke adviezen die kunnen leiden tot de weigering van een vergunningverstrekking. Zie Van den Bogert, Horsten en Tamerus (2008).

en terrorisme zijn beide zogenoemde 'gesloten subsystemen' die een vergelijkbare aanpak vergen waarin de CIE een bijzondere rol vervult en (C) in de praktijk valt er vaak moeilijk een onderscheid te maken tussen georganiseerde criminaliteit en terrorisme, waardoor beide fenomenen zowel als bedreiging van de nationale veiligheid en als criminaliteit zijn aangemerkt.

A: IGP en de bestrijding van georganiseerde criminaliteit

IGP is oorspronkelijk ontwikkeld voor de bestrijding van georganiseerde criminaliteit. Later is het, met name in de V.S., omarmd als een nieuwe manier voor politiediensten om een bijdrage te leveren aan de bestrijding van terrorisme (zie Mc Garell et al. 2007; Guidetti en Ratcliffe 2008). In tegenstelling tot 'commune' misdrijven, zoals diefstal of moord, waarbij vaak getuigen of slachtoffers het misdrijf als het ware naar de politie brengen, gaat het bij georganiseerde criminaliteit vaak om slachtofferloze delicten waarbij de politie veel meer zelfstandig op zoek moet gaan naar de delicten. Bij deze vormen van criminaliteit moet de politie dus een proactieve benadering hebben in plaats van de oude, reactieve benadering. Intelligence geeft de politiediensten een antwoord op de vraag hoe ze dat proactieve kunnen bereiken. Dit neemt overigens niet weg dat IGP inmiddels voor meer wordt gebruikt dan voor de bestrijding van georganiseerde criminaliteit en terrorisme, maar wij zijn van mening dat deze *netwidening* (het uitdijen van het begrip zodat het steeds meer omvat met het nadeel dat de onderscheidende kenmerken verloren gaan) geen positieve ontwikkeling is. De aanpak van veelvoorkomende criminaliteit of het handhaven van de openbare orde verschilt immers aanzienlijk van de bestrijding van georganiseerde criminaliteit en terrorisme. Ze vormen in dit opzicht verschillende contexten waarbinnen het concept van IGP wordt geïmplementeerd. Als een bepaald mechanisme uit een context wordt gehaald waarbinnen het succesvol is, dan wil dit nog niet zeggen dat dit mechanisme ook binnen een andere context succesvol zal zijn (zie Pawson en Tilley 2004: 55-78). Wij beperken ons onderzoek dan ook tot één context: die van de bestrijding van georganiseerde criminaliteit en terrorisme. Dit brengt ons tot de tweede reden.

B: Gesloten subsystemen

Ten tweede zijn georganiseerde criminaliteit en terroristische organisaties beide te karakteriseren als 'gesloten subsystemen' (zie Gill 2000) en ze vereisen daarom een vergelijkbare aanpak van veiligheidsdiensten en de politie. Ze schermen zich op verschillende manieren af van de overheid, hetgeen het moeilijk maakt om tot die organisaties door te dringen en informatie te verzamelen. Dit leidt ertoe dat de politie en veiligheidsdiensten gebruik moeten maken van vergelijkbare methoden voor informatieverzameling. Zo zijn voor beide diensten informanten onmisbaar.[27] De informanten zijn vaak de enigen die de diensten exact kunnen vertellen wat er plaatsvindt in de 'onderwereld'. Andere vergelijkbare middelen voor informatievergaring zijn onder andere telefoontaps en stelselmatige observatie. Het gedeelde kenmerk van al deze bijzondere inlichtingenmiddelen (AIVD) of opsporingsmethoden (politie) is dat ze heimelijk worden toegepast: het is immers niet de bedoeling dat het onderzoekssubject op de hoogte is van de informatieverzameling. De heimelijk verzamelde informatie (inlichtingen) zal vaak ook moeten worden geanalyseerd om te kunnen inschatten wat de betekenis en waarde van de informatie

[27] Deze vorm van informatie wordt '*Human Intelligence*', oftewel 'HUMINT' genoemd.

is. Het belang van analyse is met name bij gesloten subsystemen erg groot omdat deze zich door middel van het gebruiken van contrastrategieën en manipulatie actief proberen af te schermen van de veiligheidsdiensten en de politie. Deze organisaties kunnen zich verweren tegen deze manipulatie door de informatie stelselmatig en gestructureerd te analyseren. De hierboven genoemde tactieken en werkmethoden werden voorheen vrijwel uitsluitend gebruikt door de inlichtingen- en veiligheidsdiensten. Voordat deze tactieken en werkmethoden door de Amerikaanse *Drug Enforcement Agency* (DEA) in Europa werden geïntroduceerd, werd het gebruik ervan door politieorganisaties, zelfs door functionarissen van deze politiediensten, gezien als "*unnecessary, unacceptable and often illegal*" (Nadelmann 1993:192). Inmiddels zijn de tactieken en methoden ook in Europa breed geaccepteerd en een standaard onderdeel van het arsenaal van de politiële onderzoeksmethoden geworden. Ze kunnen vaak ook op andere vormen van criminaliteit worden toegepast. Dus op zichzelf ligt daarin geen reden tot de afbakening. Echter het feit dat georganiseerde criminaliteit en terrorisme van de opsporings- en inlichtingendiensten een vergelijkbare proactieve benadering vergen en andere taken (tot nu toe) een andere benadering vergen, maakt de gekozen afbakening een logische afbakening. Omdat de CIE is belast met het runnen van informanten en het analyseren van informatie hebben wij ons onderzoek afgebakend tot dit organisatieonderdeel van de politie.

C: Moeilijk van elkaar te onderscheiden

Ten derde is er niet snel een onderscheid tussen georganiseerde criminaliteit en terrorisme te maken. Het is waar dat er een verschil zal zijn in oogmerk, waarbij het criminele oogmerk gericht zal zijn op winstbejag en het terroristische oogmerk op het afdwingen van politieke en maatschappelijke veranderingen door middel van angst en geweld (Aalberts 2009: 15-18). Inderdaad, op zichzelf is dit een duidelijk onderscheid. In de praktijk is het onderscheid echter diffuus. Terroristische netwerken begeven zich niet zelden op het vlak van de georganiseerde criminaliteit en andersom. Omdat er in veel gevallen eenvoudigweg geen onderscheid kan worden gemaakt tussen georganiseerde criminaliteit en terrorisme, beperken wij ons niet tot één van beide fenomenen, maar behandelen wij beide fenomenen.

Mede omdat ze zo moeilijk van elkaar te onderscheiden zijn, zijn zowel georganiseerde criminaliteit en terrorisme in het heden en het verleden gedefinieerd als bedreigingen voor de nationale veiligheid en vormen van criminaliteit (Fijnaut 2004; Andreas en Nadelmann 2006). Terroristische aanslagen zoals die op 9-11 in New York en Pennsylvania, zijn vormen van massamoord (een misdrijf) en een aanval op de nationale veiligheid. Het doel van dergelijke aanslagen is het veroorzaken van angst en paniek in een samenleving om zo politieke veranderingen teweeg te brengen. Zodra het een bedreiging van de nationale veiligheid wordt, geldt het als aandachtsgebied van de inlichtingen- en veiligheidsdiensten. Het gekozen middel is echter ook te kwalificeren als een misdrijf: het is (massa)moord. Dit maakt terroristische organisaties tot legitiem doelwit van de opsporingsdiensten. Voorts plegen terroristische organisaties stelselmatig misdrijven om aan geld en middelen te komen, hetgeen ze vaak in het vizier van de opsporingsdiensten brengt. Criminele organisaties vormen op hun beurt een bedreiging voor democratische systemen omdat ze niet zelden gebruik maken van corruptie.

De hierboven genoemde redenen leiden ertoe dat georganiseerde criminaliteit en terrorisme voor zowel de veiligheidsdiensten als de politie legitieme aandachtsgebieden vormen. Dit maakt de bestrijding van georganiseerde criminaliteit

en terrorisme een geschikt onderzoeksveld voor ons onderzoek: beide diensten hebben een mogelijk legitieme taak en maken gebruik van vergelijkbare methoden van informatieverzameling. Ze komen elkaar bij de bestrijding van deze fenomenen tegen. Wij merken hier echter ook op dat de meeste relevante ontwikkelingen met betrekking tot ons onderzoek te maken hebben met terrorismebestrijding. Zo is er veel nieuwe wetgeving die het de opsporingsdiensten mogelijk maakt om eerder opsporingsbevoegdheden in te zetten, en zijn er nieuwe samenwerkingsverbanden tussen veiligheidsdiensten en de politie in het leven geroepen die de terrorismebestrijding in het algemeen effectiever en efficiënter moeten maken. Bij het eerste onderwerp van ons onderzoek (de implementatie van IGP in de praktijk van de CIE) leggen wij nog niet de nadruk op terrorismebestrijding: onze bevindingen zijn zowel relevant voor de bestrijding van georganiseerde criminaliteit als voor de bestrijding van terrorisme. Maar met name bij het tweede onderwerp van ons onderzoek, te weten de verhouding tussen de AIVD en de CIE, zal de meeste aandacht uitgaan naar terrorismebestrijding omdat hier de meeste ontwikkelingen plaatsvinden. Echter, ook voor dit tweede onderwerp geldt dat veel van onze praktijkbevindingen ook opgaan voor de verhouding tussen de AIVD en de CIE bij de bestrijding van georganiseerde criminaliteit. Wij hebben er daarom voor gekozen om het onderwerp niet af te bakenen tot alleen terrorismebestrijding.

1.11 De onderzoekskeuze voor Angelsaksische literatuur

Bij dit onderzoek maken we voor het theoretisch kader gebruik van een aanzienlijke hoeveelheid Angelsaksische literatuur. Hier is een aantal redenen voor. Wij geven er drie.

Allereerst moet de Angelsaksische invloed op het Nederlandse politiebestel niet worden onderschat. Zo is de oorspronkelijke Engelse term voor IGP, *intelligence-led policing,* afkomstig uit Kent, Groot-Brittannië. De Nederlandse politie kopieert in grote mate onderdelen van dit Britse concept. Zo ontwikkelt de Dienst Nationale Recherche Informatie (DNRI) het 'Nationaal Intelligence Model' (NIM); het is grotendeels een kopie van het Britse *National Intelligence Model.*

Als tweede reden noemen wij de grote Amerikaanse invloed op ontwikkelingen in het Nederlandse politiewerk in het algemeen. Met name de Amerikaanse drugsprohibitie beïnvloedt het politiewerk in West-Europa en dit heeft geleid tot verregaande veranderingen in wettelijke mogelijkheden voor de opsporing van dit type criminaliteit (Nadelmann 1993; Andreas en Nadelman 2006). De Amerikaanse politiestijlen hebben tot op de dag van vandaag een grote invloed op de Nederlandse politie[28], en de uitgebreide literatuur over deze Angelsaksische politiestijlen biedt waardevolle inzichten in de achtergrond, oorsprong en implicaties van de politiële ontwikkelingen in Nederland.

Een derde reden voor het gebruik van veel Angelsaksische literatuur heeft te maken met het andere aspect van dit onderzoek: de veiligheidsdiensten. In de VS is er sinds de jaren '60 en '70 van de vorige eeuw veel meer aandacht geweest voor het werk van deze diensten. Er zijn staats- en senaatscommissies geweest, zoals de bekende Church-commissie, die interessant studiemateriaal opleveren voor academici en andere geïnteresseerden in de inlichtingenwereld. Ook de CIA heeft een interessante website met veel (academische) publicaties over intelligence en

[28] Zeker gezien het toenemende belang van de terrorismebestrijding, waarin een al dan niet opzettelijke van de Amerikanen duidelijk aanwezig is.

inlichtingen- en veiligheidsdiensten.[29] Er is in de VS ook meer aandacht vanuit de academische wereld voor inlichtingen- en veiligheidsdiensten dan in Nederland het geval is, alhoewel er de laatste jaren ook in Nederland meer publicaties het licht zien. Het blijft echter een gegeven dat wij voor literatuur omtrent deze diensten primair op Angelsaksische literatuur zijn aangewezen.

1.12 Onderzoeksmethode

Er zijn talloze onderwerpen gerelateerd aan IGP, zoals de relatie tussen vrijheid en veiligheid. Hierover wordt ook veel gepubliceerd. Vaak worden juridische aspecten van de politie onderzocht, hetgeen met zich meebrengt dat onder andere wetgeving en jurisprudentie worden geanalyseerd.[30] Een andere veel gebruikte onderzoeksmethode is het dossieronderzoek.[31] Er is echter weinig onderzoek naar hoe de politiële concepten in de praktijk werken. In sommige gevallen gebruiken de onderzoekers ook deels methoden die inzicht zouden moeten geven in de praktijk, zoals interviews, maar vaak is dit niet het belangrijkste doel van het onderzoek (zie: Cope 2004; Koelewijn 2009: 30; Kielman 2010). Er bestaat vanwege deze primair theoretische benadering onvoldoende inzicht in de praktijk van het politiewerk. Dit geldt zeker ook voor onderzoeken naar concepten als IGP.[32] Er is echter ook een tegenwerping die wij hier in citaat weergeven: "*this programmatic theorizing is long on concepts and short on facts. The empirical evidence is generally selective, spotty and anecdotal (...)*" (Brodeur 2007: 31).

In de volgende subsecties behandelen wij achtereenvolgens onze gehanteerde onderzoeksmethode: het exploratief empirisch onderzoek (subsectie 1.12.1), de methode van de etnografie in het bijzonder (subsectie 1.12.2) en de wijze van dataverzameling, te weten literatuuronderzoek (subsectie 1.12.3) en veldwerk (subsectie 1.12.4).

1.12.1 Exploratief empirisch onderzoek

Voor IGP en de invloed ervan op de scheiding tussen veiligheidsdiensten en de politie geldt dat er meer empirisch onderzoek nodig is. Het is uiteindelijk de vraag hoe een concept als IGP in de praktijk daadwerkelijk uitpakt. Wordt de politie inderdaad proactief? Verandert er iets in de manier waarop de politie met informatie omgaat nu er meer juridische mogelijkheden zijn? De onderzoeksvraag in hoeverre de CIE volgens IGP werkt, kan pas worden beantwoord als er inzicht is in de praktijk van het CIE-werk. Ons onderzoek is in belangrijke mate verkennend. Wij proberen een bijdrage te leveren aan de empirische bewijsvoering omtrent IGP.

Omdat er nog relatief weinig bekend is over de verhouding tussen de veiligheidsdiensten en de politiële inlichtingendiensten in het kader van de bestrijding van georganiseerde criminaliteit en terrorisme, is de empirische component van deze studie zoals gezegd voor een groot deel verkennend van aard: er zijn nog weinig tot

[29] https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/index.html, gezien op 7 maart 2012.

[30] Zie Koelewijn (2009) en Kielman (2010) voor recent onderzoek naar privacy en politie.

[31] Zie Spapens (2008) voor een voorbeeld van dossieronderzoek naar de interactie tussen de georganiseerde criminaliteit en de opsporing.

[32] Zie Gill (2000), Maguire en John (2006) voor voorbeelden van deze categorie academici . Eén van de weinige onderzoeken die wel is gebaseerd op onderzoek naar de praktijk is dat van Ratcliffe en Guidetti (2008). Zie Ericson en Haggerty (1997) voor een inmiddels enigszins gedateerd etnografisch onderzoek naar de politie.

geen theorieën op dit vlak. Ook wij zullen het stadium van theorievorming niet bereiken, maar wij komen wel tot een aanzet daartoe (zie hoofdstuk acht).

Een verandering van theorie naar praktijk, of van model naar realiteit, zoals de implementatie van intelligence in de context van de politie/CIE, is een uiterst gecompliceerd proces voor wetenschappelijke analyse. Zo zijn er bepaalde aspecten van wat we hier gemakshalve de 'politiecultuur' zullen noemen die een bepalende invloed kunnen hebben op de wijze waarop IGP in de praktijk gestalte krijgt.[33]

1.12.2 Etnografisch onderzoek

Een onderzoeksmethode die inzicht kan geven in de politiecultuur en de politiepraktijk in de brede zin van het woord, is de uit de culturele antropologie afkomstige etnografische methode.

Vanwege de focus op de praktijk van de opsporing en het exploratieve karakter kiezen wij de etnografie als onderzoeksmethode. Etnografie wordt door cultureel antropologen gebruikt om culturele fenomenen, zoals rituelen en gebruiken, te onderzoeken en te interpreteren. De onderzoeker begeeft zich in het onderzoeksonderwerp en verzamelt zijn data direct uit de omgeving van het onderwerp en uit het onderwerp zelf. Hij is dus zelf het voornaamste instrument voor dataverzameling. Door middel van interviews, literatuuronderzoek maar met name participerende observatie probeert de onderzoeker het onderwerp te doorgronden en te begrijpen. De eigen ervaringen zijn hierbij van groot belang. In de criminologie wordt etnografisch onderzoek vaak toegepast op onderwerpen waar weinig over bekend is.[34] Ook de verhouding tussen veiligheidsdiensten en de politie bij het bestrijden van georganiseerde criminaliteit en terrorisme is grotendeels onbekend terrein, hetgeen de etnografie hier eveneens tot een aangewezen methode maakt. Over het deelonderwerp intelligence is nog steeds weinig bekend. Dit is zo ondanks het feit dat het een vrij oud fenomeen is. Hiervoor is een aantal redenen aan te wijzen. We noemen er twee.

Allereerst is er de verregaande mate van geheimhouding van de inlichtingendiensten. Dit is een complicerende factor voor academisch onderzoek: de geheimhouding is er primair op gericht om de methoden en informatiepositie van de dienst af te schermen van de buitenwereld. Het betekent dat geheimhouding met name geldt voor de praktijk van het inlichtingenwerk, en dat is nu juist waar dit onderzoek meer inzicht in wil verkrijgen (overigens zonder hierbij gebruik te maken van operationele informatie, zoals informatie die mogelijk leidt tot het ontdekken van de identiteit van de informant). De verregaande mate van geheimhouding van de diensten leidt tot de volgende waarschuwing van Bernard Porter aan het adres van lezers van boeken over geheime diensten: *"(...) the first rule for the reader of any book about secret services (...) is not to trust a word of it. It could all be lies and disinformation; not on the part of the writer necessarily, but on the part of the sources he is gullible enough to believe*" (Gill en Phythian 2006: 12). Dit is een reëel gevaar

[33] In een complexe organisatie, zoals de politie, is er eigenlijk geen sprake van één cultuur. De gedeelde waarden en normen bij bijvoorbeeld de Mobiele Eenheid (ME) zijn heel anders dan die van de CIE. In hoofdstuk zeven behandelen wij de voor ons onderzoek relevante elementen van de politiecultuur, en met name de CIE-subcultuur.

[34] Of zoals Ferrell en Hamm (1998: 9) het stellen: "(...) *field research remains (....) the essential research method for uncovering the situated meaning of crime and deviance, for exposing the experiential web of symbolic codes and ritualized understandings which constitute deviance and criminality*".

voor ieder boek over geheime diensten, inclusief het boek dat de lezer thans voor zich heeft.

Ten tweede lijkt het door de verregaande geheimhouding van de geheime diensten wellicht moeilijk om het onderzoek te herhalen en de uitspraken te toetsen. De toegang voor academici tot dergelijke diensten of de relevante informatie wordt immers grotendeels als beperkt ervaren.[35] Dit probleem speelt eigenlijk bij veel antropologisch onderzoek: vaak is dergelijk onderzoek formeel wel over te doen, maar gelden er praktische beperkingen die het feitelijk een stuk lastiger maken. Dit geldt echter in nog sterkere mate voor onderzoek naar geheime diensten.

Met betrekking tot het verkrijgen van toegang tot de politie hebben wij bij dit onderzoek evenwel geen probleem geconstateerd, terwijl wij door diverse collega's zijn gewezen op de moeilijkheden en barrières. Het bleek betrekkelijk eenvoudig om na een telefonisch contact en een gesprek van een paar uur een onderzoeksstage te lopen. Daarnaast zijn er inmiddels meerdere politiemedewerkers die zelf promotieonderzoek doen naar verschillende fenomenen. Zolang er geen geclassificeerde informatie wordt verstrekt, lijkt het dus mogelijk om wetenschappelijk onderzoek bij de politie uit te voeren.

Indien een onderzoeker zich beperkt tot officiële publicaties van de diensten, dan bestaat immer het gevaar van manipulatie en misleiding. Dit onderzoek probeert hier door middel van de etnografische onderzoeksmethode aan te ontkomen. De geheimhouding functioneert vooral als een barrière bij het binnenkomen in de organisatie. De toegang tot verschillende informatieafdelingen binnen het opsporingsapparaat, waaronder de CIE, was voor ons als onderzoeker (en later als personeelslid) gemakkelijk. Dit is in tegenstelling tot wat ons door andere onderzoekers is voorgehouden. Na de gebruikelijke veiligheidsonderzoeken konden wij met ons veldwerkonderzoek van start gaan. Met name de mogelijkheid om bij de CIE onderzoek te kunnen doen, is bijzonder te noemen.[36] Vanzelfsprekend hebben wij tijdens ons onderzoek op geen enkele wijze te maken gehad met informatie die bijvoorbeeld zou kunnen leiden tot het vaststellen van de identiteit van informanten. Ons onderzoek richt zich op werkprocessen en de wijze waarop IGP in de praktijk vorm krijgt, informanten-informatie is voor ons onderzoek niet relevant. Toch is het gegeven dat wij ook bij de CIE onderzoek hebben kunnen doen op zichzelf al een relevante onderzoeksbevinding: de CIE heeft geheimhouding hoog in het vaandel staan, maar is niet meer zo afgeschermd van de buitenwereld dat (wetenschappelijk) onderzoek naar bijvoorbeeld haar werkwijze niet mogelijk is.[37] Documenten en interviews konden worden beoordeeld op waarheid door gebruik te maken van

[35] Zie het proefschrift van Engelen (1995). Engelen is de enige die in het kader van zijn onderzoek naar de geschiedenis van de BVD onbeperkt toegang had tot de archieven van de BVD/AIVD. Bij dit onderzoek was er wel een aantal andere waarborgen ingebouwd, zoals de onbeperkte toegang van de commissie tot het bronmateriaal. Dit is bij een onderzoek naar fenomenen in de praktijk echter niet mogelijk.

[36] Deze afdeling staat bij de buitenwereld vaak bekend als de geheime afdeling van de politie (zie Van der Bel et al. 2009). Een CIE onderhoudt contacten met informanten, mensen die met gevaar voor eigen leven informatie verstrekken aan de politie onder voorwaarde dat hun identiteit wordt afgeschermd. De identiteit van de informanten zal door de CIE dan ook vrijwel altijd en ten koste van bijna alles worden afgeschermd. Dit leidt ertoe dat sommigen (met name journalisten en advocaten) de CIE aanduiden met 'sectie stiekem'. Zie bijvoorbeeld: het Parool *Getuige in Holleeder-zaak zegt weinig tot niets*, 18-12-2008, bron: www.hetparool.nl, gezien op 30 juni 2010. Zie ook Middelburg en Vugts (2006) en Kielman (2010: 33).

[37] De CIE is sinds de Commissie van Traa steeds transparanter geworden. Zie onder meer: Kielman (2010: 33), Van der Bel et al. (2009).

datatriangulatie. Meer hierover bij de behandeling van het veldwerk in subsectie 1.12.4.

Met name participerende observatie is een hulpmiddel tegen manipulatie: het is voor medewerkers van een organisatie erg moeilijk om gedurende twee jaar een show op te voeren zonder dat de onderzoeker daar op een gegeven moment doorheen prikt. Hier staat echter weer het gevaar van '*going native*' tegenover: de onderzoeker identificeert zich zo sterk met het onderzoeksonderwerp dat hij er deel van gaat uitmaken en daarmee zijn objectiviteit verliest. Op het eerste gezicht zal het op de lezer over kunnen komen dat dit bij mij ook is gebeurd. Voor details van de wijze waarop wij het praktijkonderzoek hebben verricht, de overstap naar de praktijk van de opsporing en hoe wij met het gevaar van *going native* zijn omgegaan verwijzen wij naar hoofdstuk zes.

Tot slot een korte opmerking over de beperking van etnografisch onderzoek. Het is namelijk onmogelijk om met behulp van de etnografische methode de situatie bij alle organisatieonderdelen van een politiekorps te onderzoeken, laat staan bij alle korpsen. Het is dus zeer goed mogelijk (en zelfs waarschijnlijk) dat er elders dan bij de door ons onderzochte onderdelen en korpsen sprake is van een andere situatie of van een andere beleving van de door ons geschetste 'werkelijkheid' door de medewerkers van het betreffende onderdeel en/of korps. Wellicht dat er in de toekomst ook bij andere afdelingen en korpsen vergelijkbaar wetenschappelijk onderzoek zal worden verricht, waardoor er uiteindelijk een breder inzicht in de praktijk van de (politiële) intelligence zal ontstaan. Dit onderzoek kan als een eerste aanzet tot een dergelijk onderzoek worden beschouwd.

1.12.3 Methode van dataverzameling 1: literatuuronderzoek

Voor de hoofdstukken drie en vier waarin respectievelijk de AIVD en de CIE worden beschreven, is primair gebruik gemaakt van literatuuronderzoek. Over de politie wordt veelvuldig gepubliceerd, en van de relevante wetenschappelijke publicaties maken we vanzelfsprekend veel gebruik. Er verschijnt tegenwoordig echter ook steeds meer over inlichtingen- en veiligheidsdiensten in het algemeen en de AIVD in het bijzonder. In het laatste decennium verschenen diverse publicaties over de AIVD, zoals *De AIVD in verandering* van de Commissie Havermans (2004). De dienst publiceert zelf ook jaarverslagen en andere documenten die voor dit onderzoek zijn geanalyseerd. Daarnaast is veelvuldig gebruik gemaakt van de publicaties van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten.[38]

Voor een onderzoek met diverse juridische aspecten gebruiken wij evenwel weinig jurisprudentie. De reden hiervoor ligt in het onderwerp van dit onderzoek. Wij onderzoeken de verhouding tussen twee overheidsdiensten en, behoudens uitzonderingsgevallen, is dit zelden het onderwerp van jurisprudentie. Het is ons voorts niet te doen om de (rechts)gevolgen van die verhouding voor externen te behandelen, en dat is waar het in de jurisprudentie wel vaak over gaat. Daar waar de jurisprudentie direct de verhouding tussen de AIVD en de CIE treft, zal deze wel worden behandeld. De jurisprudentie met een indirecte invloed op ons onderwerp laten wij zoveel mogelijk achterwege.

Voor beide diensten geldt dat er zogenoemde 'grijze publicaties' circuleren die in principe niet voor extern gebruik zijn. Hoewel er steeds meer verschijnt op het inlichtingenvlak zijn ook deze grijze publicaties van groot belang voor dit onderzoek.

[38] Zie voor alle publicaties van deze toezichthouder: www.ctivd.nl. gezien op 3 februari 2009.

Bepaalde publicaties die niet zijn bedoeld om buiten de politieorganisatie te verspreiden, zijn uitsluitend gebruikt als 'sturingsinformatie'. Dit wil zeggen dat ze de basis vormen voor bijvoorbeeld interviewvragen. Wij zullen niet direct uit deze stukken citeren.[39]

Naast de literatuurstudie liepen wij een onderzoeksstage van twee jaar bij de politie, meer specifiek bij de CIE en de RIO. De empirische vragen naar de praktijk van de verhouding tussen de diensten beantwoorden wij met behulp van de data die wij in deze periode hebben verzameld. Dit betekent dat ons onderzoek met name inzicht geeft in de perceptie van de politie. Het is namelijk niet mogelijk om een onderzoeksstage bij de AIVD te doen. Wel hebben wij gesproken met enkele (voormalige) medewerkers van de AIVD.

1.12.4 Methode van dataverzameling 2: veldwerk

Tijdens het veldwerk hebben wij twee methoden van dataverzameling gebruikt: participerende observatie en interviews. Voor de participerende observatie hielden wij gedurende het gehele onderzoek een dagboek bij. Voor de interviews hebben wij gedurende twee maanden eerst korte gesprekken met diverse medewerkers gehouden. Deze gesprekken waren ongestructureerd en hadden meer het kenmerk van verkennende gesprekken dan van daadwerkelijke interviews. Na deze gesprekken hebben wij 40 interviews gehouden met 35 ervaringsdeskundigen en experts op het gebied van de verhouding tussen de AIVD, de CIE en de RIO. Drie medewerkers hebben wij meerdere malen gesproken. Bij een groot aantal interviews (19) hebben wij hulp gehad van een stagiaire, Elen Bijl, die onder onze begeleiding een scriptie heeft geschreven over geheimhouding binnen de politie. Ook medewerkers en voormalige medewerkers van de AIVD zijn geïnterviewd. Deze interviews zijn semi-gestructureerd van aard in die zin dat bepaalde specifieke onderwerpen aan bod moesten komen. Tijdens de onderzoeksstage hebben wij ook werkzaamheden verricht voor de CIE en de RIO, veelal op juridisch vlak. Zo hebben wij in 2008 bijgedragen aan advisering omtrent de invulling van de CT-Infobox. Daar waar deze activiteiten raken aan onderzoeksrelevante onderwerpen, geven wij dat duidelijk aan. De werkzaamheden brachten ons in aanraking met diverse respondenten die wij in een later stadium hebben geïnterviewd. Bovendien leverden de werkzaamheden belangrijke nieuwe inzichten op in de wereld van de geheime diensten.

Voor de analyse van de data maken wij gebruik van datatriangulatie. Concreet betekent dit dat bevindingen uit de interviews alleen worden opgenomen in het proefschrift als hiervoor twee andere bronnen zijn. Dit kunnen bevindingen uit de participerende observatie of het literatuuronderzoek zijn, of bevindingen uit andere interviews (met andere respondenten). De analyse is dus altijd op meer dan één bron gebaseerd om te voorkomen dat de analyse anekdotisch van aard wordt.

---

[39] Een belangrijke uitzondering is de afstudeerscriptie *Bouwen aan Vertrouwen* (anoniem 2005), over de samenwerking tussen de AIVD en de CIE van de DNR. Oorspronkelijk zou dit document niet worden gepubliceerd in welke vorm dan ook, maar vanwege een misverstand heeft het een dag online op de website van de Erasmus Universiteit gestaan. Twee journalisten van het radioprogramma Argos kwamen het tegen tijdens het surfen en hebben er een radio item van gemaakt waarin de chef van de CIE van de Nationale Recherche en de Directeur Democratische Rechtsorde van de AIVD op de scriptie ingaan. Het stuk is inmiddels van de site van de Erasmus Universiteit verwijderd, maar het circuleert nog steeds op het internet. Daarmee is het een gewone bron geworden van waaruit wij dan ook vrijelijk kunnen citeren. Ga voor een html versie van 'Bouwen aan Vertrouwen' naar: http://www.onjo.nl/Item.2654.0.html?entx_ttnews[cat]=301encHash=e465c81f44entx_ttnews[tt_news]=6087entx_ttnews[backPid]=2652encHash=d9d355de10, gezien op 05 juli 2008.

1.13 Structuur van het proefschrift

In deze sectie volgt een omschrijving van de structuur van het proefschrift. In hoofdstuk één geven wij een inleiding op het onderwerp en formuleren wij de probleemstelling en de vier vraagstellingen van ons onderzoek. Daarnaast beschrijven wij onze onderzoeksmethode en lichten wij de gemaakte keuzes toe. In hoofdstuk twee behandelen wij het politieke inlichtingenwerk. Dat gebeurt aan de hand van de belangrijkste kenmerken van een veiligheidsdienst. Daarnaast geven wij vergelijkbare kenmerken van een traditionele politiedienst. Hoofdstuk twee geeft antwoord op OV 1: *Wat zijn de traditionele kenmerken van veiligheidsdiensten en de politie?* Daarnaast schetst hoofdstuk twee de belangrijkste verschillen tussen de politie en de veiligheidsdienst.

In hoofdstuk drie gaan wij in op de Nederlandse veiligheidsdienst, de AIVD. Wij schetsen onder andere de aard en functie van de dienst en behandelen de juridische- en politiek-bestuurlijke context waarbinnen de dienst functioneert. In het derde hoofdstuk werken wij de eerste onderzoeksvraag verder uit voor de Nederlandse situatie.

In hoofdstuk vier behandelen wij de organisatie van de CIE en de informatieorganisatie binnen de politie. Dit hoofdstuk werkt de algemene kenmerken van de politie verder uit voor de CIE.

Hoofdstuk vijf behandelt het concept IGP. De achtergrond en doelstellingen van dit concept worden behandeld, alsmede de relatie met conceptuele voorlopers van IGP. Ook behandelt hoofdstuk vijf een theoretisch raamwerk voor het ontstaan van IGP en voor begrip van hoe intelligence (binnen de context van de CIE) werkt. Dit hoofdstuk beantwoordt OV 2: *Wat is het concept IGP en hoe beoogt dit concept de traditionele Nederlandse CIE te veranderen?*

Hoofdstuk zes behandelt de methodologie en de onderzoekspraktijk. In dit hoofdstuk beschrijven wij de uitvoering van het praktijkonderzoek en proberen wij de lezer inzicht te geven in de wijze waarop wij tijdens het onderzoek met de bijzondere (problematische) aspecten van het etnografische onderzoek zijn omgegaan.

In hoofdstuk zeven analyseren wij de praktijk van IGP. Aan de hand van de etnografische onderzoeksmethode onderzoeken wij in hoeverre het concept van IGP in de praktijk van de Nederlandse CIE uit de verf komt. Wij benoemen de belangrijkste knelpunten en bieden hiervoor (theoretische) verklaringen. In dit hoofdstuk wordt OV 3 behandeld: *in hoeverre is IGP geïmplementeerd in de Nederlandse CIE-praktijk?*

Hoofdstuk acht behandelt de praktijkaspecten van de verhouding tussen de CIE en de AIVD. Net als in hoofdstuk zeven benoemen wij de belangrijkste knelpunten en bieden wij hiervoor (theoretische) verklaringen. Dit hoofdstuk ziet op OV 4: *Welke invloed heeft de implementatie van IGP in de context van de CIE op de verhouding tussen de CIE en de AIVD?*

In hoofdstuk negen beantwoorden wij de probleemstelling en de deelvragen.

2| Algemene kenmerken van veiligheidsdiensten en de politie

In dit hoofdstuk behandelen wij de algemene kenmerken van de veiligheidsdienst en de politie. Brodeur (2007) analyseerde de verschillende kenmerken van de diensten en maakte hierbij een onderscheid tussen een 'hoge politie' (HP, oftewel de veiligheidsdienst) en een 'lage politie' (LP, oftewel de politie) (zie ook Andreas en Nadelmann 2006; Sheptycki 2007). De hoge politie bestaat uit de moderne veiligheidsdiensten die zijn belast met het beschermen van de nationale veiligheid; de lage politie bestaat uit de politieorganisaties die zijn belast met het opsporen van strafbare feiten. Dit onderscheid tussen een hoge en een lage politie is voor het eerst aangebracht door de eerste minister van politie van Napoleon I, Joseph Fouché.[40] Zijn politie was een politieke politie die zeer dicht tegen de machthebber aan zat. Het doel was de bescherming van de machthebber en de heersende klasse. Vanwege deze positie dicht tegen de zittende macht aan, noemde Fouché dit de hoge politie. De andere taak van de politie werd vervuld door de lage politie. Deze taak was gericht op het beschermen van de gemeenschapsveiligheid, en had volgens Fouché meer te maken met '*policing the lampposts*': bij de straatverlichting trof men in Parijs vroeger de prostituees en de zakkenrollers aan (Stove 2003: 67-112; Brodeur 2007: 26). Dit betekent overigens niet dat er een groot verschil zat tussen de hoge en de lage politie als het gaat om de gehanteerde methoden. Eén van de eerste voorbeelden van een rechercheorganisatie die zich stelselmatig richtte op het opsporen van strafbare feiten (en hiervoor met name informanten gebruikte), was de Franse *Brigade de la Sureté*. Deze dienst was in 1811 opgericht door François Eugene Vidocq, zelf een voormalig veroordeelde crimineel en politie-informant (Andreas en Nadelmann 2005: 76). Toch bieden de ideaaltypen van de hoge en lage politie ons aanknopingspunten voor het behandelen van de belangrijkste verschillen tussen beide organisaties. Wij baseren ons dan ook op de inzichten van Brodeur bij de beschrijving van de veiligheidsdienst en de politie.

In dit hoofdstuk beantwoorden wij OV 1: *Wat zijn de traditionele kenmerken van een veiligheidsdienst en de politie?* De vier belangrijkste HP-kenmerken van de veiligheidsdienst worden genoemd en toegelicht. Dit zijn allereerst de bescherming van de nationale veiligheid (sectie 2.1), ten tweede het geven van voorwaarschuwingen door middel van het proactief signaleren van bedreigingen (sectie 2.2), ten derde de intelligence-cyclus als werkproces (secties 2.3, 2.4 en 2.5) en ten vierde geheimhouding (sectie 2.6). Deze vier kenmerken vormen in hoofdstuk acht een toetssteen voor de beoordeling of IGP leidt tot een verandering in de verhouding tussen de taken en werkzaamheden van de veiligheidsdienst en die van de politie.

Na behandeling van de veiligheidsdienst, behandelen wij de politie op eenzelfde wijze. Wij noemen ook de vier belangrijkste kenmerken van de politiefunctie, waarbij we beginnen met een algemene inleiding (sectie 2.7). Vervolgens komen de kenmerken van de politiefunctie aan bod. Het gaat in de eerste

[40] Fouché baseerde zich in belangrijke mate op het politie- en spionage systeem van de Pruisische keizer Joseph II (1741-90). Joseph II was met name beducht voor geheime genootschappen zoals de vrijmetselarij en de Iluminati, en gebruikte een geheime politie die, voor het eerst in de geschiedenis, systematisch alle lagen van de samenleving in de gaten hield (zie Chapman 1970: 20 e.v.; Stove 2003: 193-194).

plaats om de handhaving van de rechtsorde (sectie 2.8), in de tweede plaats waarheidsvinding (sectie 2.9), in de derde plaats het opsporingsonderzoek als werkproces (sectie 2.10) en in de vierde plaats transparantie (sectie 2.11). Deze kenmerken vormen als het ware het spiegelbeeld van de kenmerken van de veiligheidsdienst, en worden in latere hoofdstukken verder uitgewerkt voor de Nederlandse situatie. Wij sluiten het hoofdstuk af met het antwoord op OV 1 (sectie 2.12).

2.1 HP-kenmerk 1: het beschermen van de nationale veiligheid

Veiligheidsdiensten houden zich bezig met de bescherming van de nationale veiligheid: dit is de *raison d'être* van de veiligheidsdienst (Brodeur 2007: 27). De politieke politie vormt in dit opzicht het paradigma van de veiligheidsdiensten: "*it reaches out for potential threats in a systematic attempt to preserve the distribution of power in a given society*" (Brodeur 2007: 27). Deze veiligheidsdiensten zijn met name belast met het beschermen van de nationale veiligheid. Hiertoe verzamelen zij op verschillende manieren informatie die kan duiden op mogelijke bedreigingen van de nationale veiligheid. Voorbeelden van dergelijke veiligheidsdiensten zijn de Nederlandse AIVD, de Amerikaanse FBI, en de Britse MI5.

De vraag die in het kader van dit eerste kenmerk rijst, is wanneer er sprake is van nationale veiligheid. Een duidelijke, vastomlijnde definitie van nationale veiligheid is er echter niet. Wat specifiek als een bedreiging van de nationale veiligheid moet worden gezien, bepalen de diensten grotendeels zelf.[41] Overheden geven de veiligheidsdiensten voor deze beoordeling opzettelijk een grote discretionaire bevoegdheid: het wordt als onwenselijk gezien om het begrip 'nationale veiligheid' uitgebreid te omschrijven, omdat wat hieronder valt van tevoren vaak niet goed in te schatten is.[42] De diensten hebben deze ruimte nodig om daadwerkelijk de nationale veiligheid te beschermen en niet te verzanden in definitiekwesties die tijdig en adequaat handelen van de diensten bemoeilijken. Dit maakt het ook bijzonder lastig om aan te geven wanneer er precies sprake is van 'nationale veiligheid' en wanneer niet. Er is eenvoudigweg geen duidelijke, alomvattende definitie mogelijk.

Voor een begrip van de term 'nationale veiligheid' dienen we te rade te gaan bij concrete nationale stelsels. De Nederlandse invulling van nationale veiligheid komt in hoofdstuk drie over de AIVD aan bod. Die invulling kan namelijk het beste worden geanalyseerd vanuit de context van een specifieke dienst. Het zou te gedetailleerd zijn voor dit hoofdstuk. Maar met het oog op de in dit hoofdstuk behandelde algemene kenmerken van de veiligheidsdiensten en de politie (HP-kenmerken en LP-kenmerken), is het allereerst van belang te constateren dat (A) de kern van 'nationale veiligheid' in de praktijk neerkomt op het beschermen van de nationale politieke status quo tegen bedreigingen van buitenaf. Daarnaast stellen wij vast (B) dat in dit politieke element ook een gevaar schuilt.

A: Bescherming van de politieke status quo

In een democratische rechtsstaat betekent bescherming van de politieke status quo dat de democratisch gekozen regering (maar ook de andere democratische instituten zoals

[41] Zie voor een analyse van de juridische kwalificatie van nationale veiligheid in de Nederlandse situatie hoofdstuk drie van dit proefschrift.

[42] Het begrip '*national security*' speelt ook een rol in Straatsburgse jurisprudentie. Zie Loof (2005) voor een analyse van de Straatsburgse elementen van dit begrip.

een parlement) zoveel mogelijk worden beschermd tegen bedreigingen van buitenaf, waarbij 'buitenaf' volgens ons moet worden gezien als 'van buiten de grenzen van de democratische rechtsstaat'. Indien de politieke status quo op een wijze wordt aangetast die in een democratische rechtsstaat volstrekt geoorloofd en legitiem is, zoals door parlementaire verkiezingen, dan is er voor de veiligheidsdiensten in democratische rechtsstaten geen ruimte om op te treden. Dit geldt ook voor 'aanvallen' op de politiek door de media: media die de politiek onderzoeken en het publiek informeren vormen een belangrijke onderdeel van een democratische rechtsstaat.[43] Pas wanneer deze activiteiten buiten de grenzen van een democratische rechtsstaat vallen, bijvoorbeeld door het gebruiken van geweld, zijn de diensten gelegitimeerd om hiertegen op te treden. Het handhaven van de politieke status quo door deze te beschermen tegen illegale aanvallen is één van de 'politieke' elementen van de veiligheidsdiensten, en hetgeen waarmee de veiligheidsdiensten zich onderscheiden van de politie. Dit heeft ook consequenties voor de verhouding tussen veiligheidsdiensten en de politie. Indien de politie zich gaat bezighouden met het beschermen van een politieke status quo, begeeft ze zich op het terrein van de veiligheidsdiensten. Het lastige is overigens dat mogelijke aantastingen van de nationale veiligheid dikwijls door middel van strafbare feiten gebeurt, zoals het beramen of plegen van een terroristische aanslag. De scheidslijn tussen het domein van de veiligheidsdiensten en het domein van de politie is dan ook niet altijd even gemakkelijk te trekken.

De activiteiten die een bedreiging vormen voor de politieke status quo, zijn niet zelden ook zelf politiek van aard. Hierin komt het politieke van het inlichtingenwerk van de veiligheidsdiensten eveneens tot uitdrukking. Dit is als het ware een soort spiegelbeeld van de bovenstaande handhaving van de politieke status quo. Een voorbeeld is het lidmaatschap van een communistische partij: op zichzelf is dat niet verboden, maar er zou van de achterliggende communistische ideologie een bedreiging uitgaan voor de democratie in het geheel, zo was althans de gedachte tijdens de Koude Oorlog.[44] Bij deze onderwerpen worden democratisch gelegitimeerde wegen gebruikt voor niet-democratische doeleinden, en daarom beschouwen wij dit ook als bedreigingen van buitenaf. Dit maakt het optreden van veiligheidsdiensten echter ook problematisch.

De grens tussen het legitiem nastreven van politieke of maatschappelijke veranderingen door middel van het benutten van democratische rechten en vrijheden en het misbruiken hiervan voor ondemocratische doeleinden is van tevoren vaak moeilijk te trekken. De diensten kunnen dit zelf dikwijls ook niet en verwerven daarom noodgedwongen een informatiepositie die mogelijk ook de goedwillende burger kan treffen. Dit (volstrekt legitieme) optreden van de veiligheidsdiensten heeft als neveneffect dat het (eveneens volstrekt legitieme) optreden van burgers op een bepaalde manier wordt beknot en rechten worden geschonden. Wij geven ter illustratie een Nederlands voorbeeld. De BVD heeft tijdens de Koude Oorlog vrijwel alle communistische organisaties in Nederland gepenetreerd en daarbinnen agenten

[43] Zie voor recente Nederlandse voorbeelden van het spanningsveld tussen de media en veiligheidsdiensten in een democratische rechtsstaat het tappen van de telefoons van twee journalisten van de Telegraaf door de AIVD omdat ze over mogelijke staatsgeheimen zouden beschikken. Het gebruik van dit bijzonder inlichtingenmiddel is door de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten kritisch beoordeeld. Zie CTIVD (2009).

[44] Communisme was gedurende de Koude Oorlog (hetgeen de belangrijkste periode voor inlichtingen- en veiligheidsdiensten in het algemeen is geweest: zie Gill en Phythian 2006: 16) het belangrijkste doelwit van westerse inlichtingen- en veiligheidsdiensten, waaronder de Nederlands BVD (Engelen 1995; 2007).

geplaatst. Dit geldt ook voor politieke partijen als de Communistische Partij Nederland (CPN) (Engelen 1995; Vos et al. 2005: 31; Engelen 2007). Alhoewel destijds het communisme als een grote bedreiging werd gezien, valt niet te ontkennen dat de CPN een legitieme politieke partij was (Vos et al. 2005: 36-38).[45] De BVD heeft derhalve sturing gehad in een politieke partij die het als een bedreiging voor de nationale veiligheid beschouwde, en hiermee is ook de vrijheid van burgers beknot.

Vanwege de aard van het politieke inlichtingenwerk staan veiligheidsdiensten in nauwe relatie tot de politiek. De diensten staan daarnaast onder controle van de politiek. In de praktijk kan de politiek druk uitoefenen op de diensten, onder meer door het vaststellen van de inlichtingenagenda (de prioriteitenstelling) van de diensten. Het zijn namelijk dikwijls de belangen van de politiek die de agenda voor de diensten vaststellen. Politieke inlichtingen zijn dus grotendeels toegesneden op de politiek, vandaar ook het bijvoeglijk naamwoord 'politiek' (Wirtz 2007).

B: Het gevaar van het politieke element

Deze relatie tussen de politiek en veiligheidsdiensten is echter wel problematisch. De veiligheidsdiensten zijn namelijk vaak dienstbaar aan de politiek, en dit kan voor deze diensten nadelige gevolgen hebben. Een veiligheidsdienst wordt geacht de beleidsmakers (politici) te ondersteunen in het ontwikkelen en uitvoeren van beleid door een objectieve weergave van relevante feiten te presenteren (Wirtz 2007 a). Deze diensten zijn echter ook vaak in een bepaalde mate afhankelijk van de politiek: ze maken deel uit van de overheid en zijn van de politici die zij adviseren afhankelijk, bijvoorbeeld voor hun budgetten. In sommige gevallen worden ze dus direct aangestuurd door politici, in andere gevallen is de afhankelijkheid bijvoorbeeld een geldkwestie. Hoe ver deze verwevenheid gaat, verschilt van land tot land, en ook binnen landen zelf fluctueert de verwevenheid gedurende de tijd.[46]

De veiligheidsdiensten zijn dus in zekere mate afhankelijk van de politiek; politieke agenda's en belangen van de beleidsmakers en politici bepalen vaak de agenda van de diensten, en daar is op zichzelf niets mis mee (Gill en Phythian 2006;

[45] In de VS ging men tijdens de McCarthy-periode overigens nog een stuk verder. Daar is daadwerkelijk sprake geweest van een klopjacht op mogelijke communisten. Carrières en levens van veel burgers zijn door het optreden van de McCarthy-commissie geschaad. Het informantennetwerk van senator McCarthy bestond voor een groot deel overigens uit voormalige medewerkers van de CIA en ook de federale opsporingsdienst, de FBI, heeft onder de baas van de FBI destijds, J. Edgar Hoover, een belangrijke rol gespeeld bij de communistenjacht (Weiner 2007: 127-128). De CIA was echter zelf niet betrokken bij de communistenjacht van McCarthy. Dat gold niet voor de binnenlandse veiligheidsdienst, de FBI. McCarthy en Hoover hadden beiden een hekel aan de CIA en communisten (en aan homoseksuelen). In deze gezamenlijke vijanden vonden ze elkaar, en de FBI heeft een belangrijke bijdrage aan de onderzoekscommissie van McCarthy geleverd (zie Jeffreys-Jones 2007: 157 e.v.).

[46] Wirtz (2007) schetst een aantal verschillende 'scholen' met betrekking tot de mate van de onafhankelijkheid van intelligence ten opzichte van de politiek. In de school van Sherman Kent wordt er zoveel mogelijk objectiviteit betracht. Contact tussen de politieke opdrachtgevers en afnemers moet waar mogelijk worden voorkomen. Dit gebeurt om de onafhankelijkheid van de veiligheidsdienst te garanderen. Het latere hoofd van de inlichtingendienst CIA, Robert Gates, was echter van mening dat intelligence-producten bruikbaar moeten zijn voor de politiek. Hij vond een nauwe relatie met de politieke opdrachtgevers en afnemers van intelligence juist positief, omdat de inlichtingendienst op die manier beter in staat is om het intelligence-product af te stemmen op de wensen van de afnemer, zonder dat de objectiviteit geweld aangedaan mocht worden. Hetzelfde geldt voor de veiligheidsdienst (zie sectie 1.2 voor het verschil tussen de inlichtingendiensten en de veiligheidsdiensten). Voor beide scholen is wel iets te zeggen, maar dat het risico voor het politiceren van intelligenceproducten bij de laatste school het grootst is, mag duidelijk zijn.

Johnson 2007). Veiligheidsdiensten moeten immers wel bruikbare inlichtingenproducten produceren en ze dienen de beleidsmakers en politici te helpen bij het formuleren en uitvoeren van beleid op die gebieden welke zij van belang achten (Wirtz 2007a: 142-144; Hedley 2007: 131-133). Een veiligheidsdienst verliest zijn waarde op het moment dat de onderwerpen van de geleverde inlichtingen niet overeenkomen met de politieke agenda's van de beleidsmakers en politici.

Andersom is de politiek ook afhankelijk van de veiligheidsdiensten. Deze diensten geven de politiek vaak onmisbare informatie en inzichten in de problematiek waarmee politici worden geconfronteerd. Veiligheidsdiensten en de politiek zijn dan ook wederzijds afhankelijk van elkaar. Hierin schuilt een risico voor de veiligheidsdiensten. De wederzijdse afhankelijkheid van de politiek en de veiligheidsdiensten kan er namelijk toe leiden dat de politieke belangen en agenda's niet alleen de inlichtingenagenda, maar ook de uitkomsten van het inlichtingenproces gaan bepalen. De inlichtingen vormen dan niet langer een objectieve weergave van feiten, maar worden gekleurd door de politieke wensen van de ontvanger ervan. Politieke inlichtingen verliezen hiermee hun waarde op de lange termijn: een beeld van de werkelijkheid dat niet overeenkomt met de realiteit kan snel leiden tot ineffectief overheidsbeleid. Een goed voorbeeld van hoe de politiek de (inlichtingen-en) veiligheidsdiensten kan beïnvloeden, is de aanloop naar de oorlog in Irak (Gill en Phythian 2006: 125-147).

2.2 HP-kenmerk 2: voorwaarschuwingen en proactief signaleren van bedreigingen

Na een terroristische aanslag of een andere gebeurtenis waarbij belangen van nationale veiligheid in het geding zijn, rijst vaak de vraag of de gebeurtenis voorkomen had kunnen worden. Dikwijls wordt er dan gekeken naar de veiligheidsdiensten die het gevaar vroegtijdig hadden moeten signaleren en voorkomen. In dergelijke situaties wordt een terroristische aanslag vaak voorgesteld als het gevolg van het falen van een veiligheidsdienst (zie Turner 2006). Vanwege de belangen die zijn gemoeid met het beschermen van de nationale veiligheid, dienen bedreigingen voorkomen te worden. Veiligheidsdiensten kunnen niet afwachten totdat een mogelijke bedreiging van de nationale veiligheid werkelijkheid is geworden. Omdat in de meest extreme gevallen het voortbestaan van de democratische rechtsstaat in het geding is, zullen de veiligheidsdiensten altijd proberen om zo vroeg mogelijk een dreiging te onderkennen zodat deze tijdig kan worden weggenomen.

Fouché was al doordrongen van het belang van voorwaarschuwingen voor zijn hoge politie: "*everything can be known, foreseen and forestalled; carefully placed in public places, (the High Police) must be able to recognize agitators, and take by surprise any treason which is being prepared*" (Brodeur 2007: 29). Tot op de dag van vandaag ligt de kracht van inlichtingen (en intelligence) bij de veronderstelde voorspellende waarde: "*if intelligence is worth having, it is because analysis will provide customers with prior warnings of potential developments (that is, potential surprises) affecting their security/relative advantage*" (Gill en Phythian 2006: 6). Deze vermeende capaciteit om voorwaarschuwingen te genereren is evenwel ook een problematisch onderdeel van het verzamelen van inlichtingen. Sceptici zullen zeggen dat het giswerk is, en dat het proces van analyse de waarschijnlijkheid van een concrete voorspelling slechts tot op een zekere hoogte kan inschatten: "*more of a particular type of input will not alter the basic fact that intelligence can deal only in probabilities, and (...) the range of variables that can be generated by human*

interaction or introduced by different, subjective analysis of a given situation will always serve to limit the utility of intelligence work and to limit its predictive power to well below 100 per cent" (Gill en Phythian 2006: 15). Hoe langer de periode waarop de voorspelling betrekking heeft, des te waarschijnlijker dat de variabelen veranderen en des te groter de kans dat de voorspelling onjuist blijkt te zijn. Dit geldt voor alle voorspellingen, dus ook voor voorspellingen in de veiligheidssector. Turner noemt dit het '*uncertainty principle*' en acht het veronderstelde voorspellende karakter van het inlichtingenwerk zelfs de grote boosdoener achter het falen van zowel de inlichtingendiensten als de veiligheidsdiensten (Turner 2006: 111). In zijn optiek zijn inlichtingen- en veiligheidsdiensten gedoemd om periodiek te falen: de toekomst is te complex en ook de inlichtingen- en veiligheidsdiensten kunnen niet alles weten. Dit laat echter onverlet dat er van deze diensten wordt verwacht dat zij zo vroeg mogelijk een dreiging onderkennen en voorkomen. De vraag die nu rijst is op welke manier een veiligheidsdienst tot zijn voorspellingen komt. Hier is geen eensluidend antwoord op te geven. De lezer krijgt wellicht een idee van de voorspellende werkzaamheden van het inlichtingenwerk aan de hand van twee voorbeelden van hoe diensten dit in de praktijk doen, te weten (A) de traditionele trend- en fenomeenonderzoeken en (B) de meer technisch hoogstaande *profiling* en *datamining*. Hieronder bespreken we beide voorbeelden.

A: Fenomenen- en trendonderzoeken

Een traditionele methode van de veiligheidsdienst is het in kaart brengen van brede sociaal-maatschappelijke ontwikkelingen en fenomenen en het identificeren van trends. Deze trends kunnen worden doorgetrokken naar de toekomst en, onder het gelijk blijven van de relevante variabelen, kan een veiligheidsdienst een verwachting uitspreken over toekomstige ontwikkelingen. Zo produceerde de BVD in het begin van de jaren '90 van de vorige eeuw een visiedocument waarin de dienst stelde dat de verdergaande radicalisering en fundamentalisering van moslimgemeenschappen in het buitenland een weerslag kon krijgen op de verhoudingen tussen migrantengroepen in Nederland en hun houding ten opzichte van de Nederlandse samenleving. De dienst zou nog herhaaldelijk in jaarverslagen en andere documenten aandacht vragen voor dit onderwerp. De BVD zag het moslimfundamentalisme dus al ver voor de aanslagen van 11 september 2001 als een potentieel gevaar (Abels 2007: 124; zie ook Abels en Willemse 2004: 87-88). Dit is een voorbeeld van een traditionele inlichtingenanalyse zoals die al jarenlang door de diverse diensten wereldwijd wordt gedaan. Met de ontwikkelingen van de technologie zijn er echter nieuwe methoden en technieken die wellicht meer tot de verbeelding zullen spreken.

B: Geautomatiseerde profiling en datamining

Twee essentiële technieken die nauw aan elkaar verwant zijn (maar bepaald niet hetzelfde), zijn (B1) geautomatiseerde *profiling* en (B2) *data-* en *text-mining*. Deze technieken kunnen worden gevat onder de noemer *E-Discovery. E-Discovery* heeft een tweeledige doelstelling: (1) elektronische data veiligstellen die mogelijk van belang zijn in een onderzoek, en (2) het in die data ontdekken van gegevens die van belang zijn voor het onderzoek, danwel aantonen dat bepaalde informatie niet aanwezig is (Henseler 2010: 20). Hieronder lichten we de beide technieken (B1 en B2) kort toe.

B1: Geautomatiseerde profiling

Door middel van *profiling* probeert men in een vroeg stadium mogelijke dreigingen te onderkennen door veel gevallen te vergelijken en overeenkomsten te verzamelen. Deze overeenkomsten worden gecombineerd en leveren een profielschets op. Bij *profiling* wordt bijvoorbeeld gekeken naar de kenmerken van veel verschillende (vermoedelijke) terroristen. Waar komen ze vandaan? Wat zijn uiterlijke kenmerken die opvallen? Zijn er gedragsanalyses beschikbaar? Deze verschillende kenmerken worden vervolgens geïnterpreteerd om de meest relevante kenmerken en indicatoren te identificeren en aan de hand hiervan schetst een dienst een beeld van de ideaaltypische terrorist: de profielschets. Deze profielschets wordt vervolgens gedigitaliseerd en aan de hand van het profiel zoekt de dienst door databanken op zoek naar onbekende individuen die aan een groot deel van de kenmerken uit de profielschets voldoen. Bij een *hit* (iemand die aan de profielschets voldoet) wordt deze persoon geselecteerd voor een verdere controle.[47] Een voorbeeld van geautomatiseerde *profiling* is het CAPPS II project in de Amerikaanse burgerluchtvaart. Aan de hand van profielen wordt in de databanken van de luchtvaartmaatschappijen gezocht naar potentiële terroristen.[48]

Nieuwe *profiling*-systemen in Nederland worden ontwikkeld in het kader van het KIM-project (Kennis In Modellen), waaraan verschillende partners uit de veiligheidssector deelnemen. Eén van de projecten heeft als doel het in een vroeg stadium detecteren van radicalisering, onder andere aan de hand van een lijst van indicatoren; dit is eveneens een vorm van *profiling*. Dat *profiling* helemaal geen nieuw fenomeen is, blijkt overigens uit de toepassing van de techniek door Duitsland ten tijde van de RAF-terroristen. Het werd toen *Rasterfahndung* genoemd, en bestond uit het vergelijken van een groot aantal kenmerken van mogelijke terroristen (zie: Muller, Spaan en Ruitenberg 2004: 175-176; Muller en Petit 2008: 293). Het gaat echter te ver om hier dieper op in te gaan.

B2: Data- en text-mining

In een samenleving die kan worden gekenmerkt als een 'informatiemaatschappij' verzamelen veiligheidsdiensten ongelooflijke hoeveelheden informatie. Het is echter een reëel gevaar voor deze diensten dat ze zoveel informatie verzamelen dat het niet meer allemaal kan worden bekeken en verwerkt. Deze data-overload is één van de grote problemen voor onder andere politieorganisaties (Sheptycki 2004). Een techniek om de informatieverzameling en -verwerking af te stemmen op de immer groeiende informatiestromen heet *knowledge discovery in databases*, beter bekend als *datamining*. Deze techniek is in staat om heel snel grote hoeveelheden gestructureerde data te doorzoeken naar voor de zoeker relevante data. Zo kan *datamining* de kenmerken zoeken die bijvoorbeeld van belang zijn voor het opstellen van een profiel in het kader van de hierboven genoemde *profiling*. Amerikaanse veiligheidsdiensten gebruiken *datamining* onder meer om in databanken met gestructureerde digitale

[47] Zie voor een theoretische benadering van *profiling* en surveillance Ogura (2006).

[48] Formeel zou het CAPPS systeem zijn gestopt, maar er zijn aanwijzingen dat vergelijkbare systemen nog draaien. Bruce Schneier, een gerenommeerd veiligheidsexpert, is bijzonder kritisch over geautomatiseerde *profiling*. De kern van zijn kritiek is dat de vals positieven en vals negatieven veel te hoog liggen omdat er te weinig terroristen zijn aan de hand waarvan je een profielschets kunt opstellen (de zogenoemde '*base rate falacy*'). Zie: www.schneier.com, gezien op 21 juli 2010. Zie ook: Heuer (1999: 157-160).

communicatie te zoeken naar terrorismegerelateerde informatie. Bijvoorbeeld het e-mail verkeer wordt dan doorzocht op termen als 'bom' of 'Bin Laden' en iedere e-mail met deze termen wordt onderschept door de diensten. Dit levert overigens ook al gigantische hoeveelheden onderschepte informatie op, welke ook moet worden verwerkt en beoordeeld op daadwerkelijke waarde voor de diensten.

Naast *datamining* bestaat er ook de techniek van *text-mining*. *Text-mining* is gericht op het doorzoeken van grote bestanden van ongestructureerde data (Scholtes 2009). Het gaat dan bijvoorbeeld om teksten in e-mails en losse foto's die niet in een relationele databank zijn opgeslagen. Deze ongestructureerde data zijn moeilijk te doorzoeken, zeker wanneer je niet weet wat je precies zoekt. Met behulp van *text-mining* kan worden gezocht naar taalkundige patronen van woorden, "*dit is dus zoeken op een hoger niveau*" aldus Scholtes (2009: 11).

Het gaat hier te ver om dieper op *datamining* en *text-mining* in te gaan, het doel is in deze sectie enkel om de lezer een idee te geven van welke moderne technieken door de veiligheidsdiensten worden toegepast.[49]

2.3 HP-kenmerk 3: de intelligence-cyclus

In deze sectie gaan wij in op HP-kenmerk drie: de wijze waarop het intelligenceproces bij de veiligheidsdiensten is gestructureerd. De mate waarin intelligence wordt geïmplementeerd in de politiepraktijk zullen wij mede aan de hand van de zogenoemde intelligence-cyclus beoordelen. Wij staan dan ook langer stil bij de intelligence-cyclus dan bij de andere kenmerken.

De intelligence-cyclus kent de volgende fasen: (1) het opstellen van een intelligence-agenda (*requirements*), (2) planning en opdracht, (3) het verzamelen van inlichtingen, (4) het verwerken van inlichtingen, (5) analyse, en (6) het verspreiden van analyseproducten. Dit kan leiden tot het bijstellen van de inlichtingenbehoeften van de klant en het opstellen van een nieuwe intelligence-agenda; daarmee is de cyclus rond. Deze weergave van het intelligenceproces kent echter tekortkomingen waar wij in de volgende sectie op zullen in gaan. De intelligence-cyclus wordt visueel voorgesteld als in figuur 2.1.

Figuur 2.1: De Intelligence-cyclus. Bron: www.fbi.gov, gezien op 19 december 2009

[49] Zie voor een overzicht van *datamining* en de implicaties voor de privacy van burgers: Custers (2004).

Hieronder werken wij de fasen van de cyclus kort uit. De fasen van verzamelen en analyseren krijgen meer aandacht dan de rest. In deze fasen onderscheidt de veiligheidsdienst zich van andere organisaties. Zij vormen op die punten de twee belangrijkste pijlers van het inlichtingenwerk.

Opstellen van een intelligence-agenda

Intelligence is ideaaltypisch een gecoördineerde activiteit. Het verzamelen van informatie en andere relevante activiteiten geschiedt niet willekeurig, maar wordt gestuurd door een bepaalde behoefte. Er is namelijk veel te veel informatie die potentieel interessant is voor de veiligheidsdienst. Intelligence-producten moeten relevant zijn voor de politici, beleidsmakers en anderen die er hun activiteiten op baseren; zij worden ook wel de 'klanten' van de organisatie genoemd. Deze klanten hebben behoefte aan adviezen op specifieke onderwerpen en zorgen daarmee voor een specifieke vraag naar intelligence-producten. Deze behoefte wordt verwoord in een 'intelligence-agenda': een soort programma van eisen (het is wellicht beter om te spreken van 'wensen' in plaats van 'eisen').

Planning en opdracht

De wens van de klant moet worden omgevormd in een concrete opdracht aan een veiligheidsdienst, iets wat de diensten over het algemeen zelf doen. De veiligheidsdiensten verzorgen daarna het aanbod van intelligence-producten. Dit begint met het verzamelen van inlichtingen.

Verzamelen

Veiligheidsdiensten richten zich op het in kaart brengen van ongekende dreigingen. Om dit te kunnen doen, hebben deze diensten een goede informatiepositie nodig. Sterker nog: het opbouwen en in stand houden van een informatiepositie is voor de diensten feitelijk een doel op zichzelf. Bij veiligheidsdiensten draait alles om het verzamelen en analyseren van informatie uit verschillende bronnen, zodat ze een goed advies aan andere partijen kunnen geven of zelf kunnen ingrijpen (Gill en Phythian 2006: 64-65; Sims 2007: 142). Dit laatste is overigens vaak een laatste redmiddel voor de diensten.[50] Eén van de belangrijkste manieren voor het verzamelen van inlichtingen door de veiligheidsdiensten is het gebruik van informanten en agenten, in het inlichtingenjargon ook wel *human intelligence* (HUMINT) genoemd. Een andere belangrijke vorm van intelligence is de zogenaamde *Signal Intelligence* (SIGINT). Vanwege het belang van deze wijzen van informatieverzameling behandelen wij (A) HUMINT en SIGINT apart. Daarna behandelen wij de (B) *Open Source Intelligence* (OSINT), minstens even belangrijk voor het intelligencewerk, maar in de literatuur vaak veel minder uitgebreid behandeld dan HUMINT en SIGINT.

[50] Dit geldt helemaal in relatie tot strafrechtelijk optreden: het verzamelen van informatie en produceren van dreigingsinschattingen en andere intelligence-producten zijn voor de veiligheidsdiensten belangrijker dan waarheidsvinding in het kader van een strafrechtelijk opsporingsonderzoek. Voor een overzicht van wat diensten doen met de informatie zie Gill en Phythian (2006: 95-101).

A: HUMINT en SIGINT

De veiligheidsdiensten maken onder andere gebruik van informanten en agenten (spionnen) om inlichtingen te verzamelen. Volgens Brodeur zijn informanten "*not only (…) the most intrusive instrument of surveillance, (…) it is also the most destructive of the social fabric as it thrives on betrayal and fosters mutual suspicion and demoralization*" (Brodeur 2007: 28). Dit blijkt met name bij totalitaire regimes, zoals de Soviet-Unie en de DDR: "*To an extent still insufficiently perceived in the West, Soviet Communism was domestic surveillan*ce." (Stove 2003: 5). Een lange tijd was het werken met informanten en '*agents provocateur*' een typisch kenmerk van het politieke inlichtingenwerk van de veiligheidsdiensten (Marx 1974: 402-442).

Veiligheidsdiensten maken echter gebruik van uitgebreide surveillance van de samenleving om zo vroeg mogelijk relevante informatie en inlichtingen te verkrijgen, en dit beperkt zich al lang niet meer tot de informanten en agenten. Zo verzamelen veiligheidsdiensten via communicatiesatellieten en het internet grote hoeveelheden informatie, de zogenoemde technologische '*signals intelligence*' (SIGINT). Een andere vorm van informatieverzameling betreft de verzameling van geografische gegevens (onder andere door middel van satellieten), de zogenoemde 'GEO-SPATIAL intelligence'. Deze technologische intelligence-benaderingen zijn lange tijd erg populair geweest binnen de inlichtingenwereld. De laatste jaren realiseren de diensten zich steeds meer dat de HUMINT inzichten kan geven die bijvoorbeeld de SIGINT niet kan (en andersom).

Al met al zijn er dus veel verschillende manieren waarop een veiligheidsdienst aan informatie komt. Een andere informatiebron is voor de veiligheidsdienst buitengewoon belangrijk en verdient daarom net als HUMINT een aparte behandeling: de *Open Source Intelligence*, oftewel OSINT.

B: OSINT

Vandaag de dag is verreweg het grootste deel van de informatie van de diensten afkomstig van zogenaamde 'open bronnen', zoals het internet en andere media. Volgens sommigen is meer dan 90 procent van de informatie afkomstig uit dergelijke open bronnen (Gill en Phythian 2006: 63-64; Johnson 2007: 2). Steele stelt dat deze OSINT 80 procent van de huidige mankracht en budget zal overnemen van de geheime operaties en dat dit uiteindelijk nog een veel beter rendement zal opleveren ook (1000 keer beter volgens Steele (2007: 95-96; 106).

De rol van deze open bronnen voor de intelligenceproducten van de inlichtingen- en veiligheidsdiensten moet echter niet worden overschat. Dat de informatie 'op straat ligt', betekent immers nog niet dat de kennis die eruit wordt opgedaan ook gemeengoed is. Het gaat namelijk niet alleen om het verzamelen van de informatie, maar ook om wat er met die informatie wordt gedaan. De verwerking van de informatie, de productie van kennis, is minstens zo belangrijk als de verzameling van informatie. Dit komt later nog aan bod bij de behandeling van analyse. Bij surveillance door de veiligheidsdiensten moet dus ook in ogenschouw worden genomen dat deze diensten op een andere manier naar informatie kijken, anders dan bijvoorbeeld bedrijven of andere overheidsinstellingen. Daarnaast is het waarschijnlijk dat bepaalde informatie over specifieke onderwerpen alleen maar verkregen kan worden door middel van geheime surveillance en spionage door middel van informanten en agenten (Gill en Phythian 2006: 63-64). In dit opzicht maken de geheime inlichtingen misschien slechts 20 procent van alle informatie uit, maar het is

deze 20 procent die wellicht juist de veiligheidsdienst meerwaarde geeft over andere 'partijen'. Dit verklaart waarom de intelligence-analisten van de CIA geheime informatie boven de andere soorten verkiezen (Johnston 2005: 24-25). Met het toenemende belang en de groei van ICT in de samenleving in het algemeen zal het belang van OSINT (en SIGINT) echter steeds meer toenemen.

Verwerken

De in de voorgaande fase verzamelde inlichtingen moeten worden verwerkt. Afgeluisterde gesprekken worden voor zover ze relevant zijn verwerkt in tekstdocumenten en indien nodig worden ze vertaald. In deze fase vindt vaak ook al een eerste verificatie van de informatie plaats. Zo kan er worden gekeken of een informant in het verleden betrouwbaar is gebleken of niet. Deze fase lijkt in eerste instantie misschien met name een administratieve handeling en daarmee in het kader van ons onderzoek weinig interessant, maar in de praktijk is dit een essentiële fase voor de veiligheidsdienst. Een moderne veiligheidsdienst verzamelt immers grote hoeveelheden gegevens die allemaal op een juiste manier moeten worden verwerkt. In deze verwerkingsfase worden gegevens geordend, hetgeen van groot belang is voor de volgende fasen van het inlichtingenwerk. Zonder ordening raken inlichtingen die mogelijk essentieel zijn verloren in de grote brij van informatie die de organisatie binnenkomt. Het is voor de inlichtingenofficier of de analist dan veel moeilijker en tijdrovender om gegevens die nodig zijn voor operaties of analyses te ontsluiten.

De fase van de verwerking ligt ten grondslag aan één van de grootste problemen van veiligheidsdiensten, te weten *stovepiping*, oftewel verkokering (zie Sheptycki 2004). In de fase van verwerking dient namelijk beoordeeld te worden welke inlichtingen van belang zijn voor welke afdeling of welk onderwerp. Vanwege veiligheidsoverwegingen bestaan er schotten tussen de verschillende informatiesystemen van de verschillende diensten en afdelingen waardoor er geen vrije uitwisseling van informatie plaatsvindt. Tijdens de fase van verwerking worden de inlichtingen in een bepaalde koker gestopt. Tussen de kokers vindt doorgaans weinig informatie-uitwisseling plaats, en de kans is groot dat informatie in de eerst gekozen koker blijft. Het is daarom van groot belang dat er een goede afweging wordt gemaakt waar welke informatie wordt weggezet. Overigens is het te eenvoudig om de fase van verwerking te positioneren tussen de verzameling van inlichtingen en de analyse ervan. Feitelijk zal informatie permanent worden verwerkt en zijn er afdelingen die een dagtaak hebben aan het schonen van bestanden (het verwijderen van informatie die onjuist, onrechtmatig verkregen of irrelevant is) en andere vormen van verwerking.

Analyseren

Analyseren is de fase waarin aan de verzamelde informatie betekenis wordt gegeven (Gill en Phythian 2006: 3; Hedley 2007). Analisten beoordelen informatie door informatie te vergelijken en in een context te plaatsen. Door middel van analyse wordt informatie omgevormd tot bruikbare kennis. De analyse is dan ook het kernproces voor het produceren van bruikbare intelligence-producten. Analyse is één van de belangrijkste activiteiten van een veiligheidsdienst, maar de vraag is wat er precies onder kan worden verstaan. Er zijn veel definities van intelligence-analyse te geven, maar wij gebruiken de definitie die wordt gebruikt in het (enige) etnografische onderzoek naar de analysecultuur bij de CIA (Johnston 2005: 4): "*the application of*

individual and collective cognitive methods to weigh data and test hypotheses within a secret socio-cultural context". Analyse is dus de primaire intellectuele activiteit van de inlichtingen- en veiligheidsdienst.

Er wordt meestal een onderscheid gemaakt tussen verschillende vormen van analyse. Zo kennen we (1) de operationele analyse, (2) de tactische analyse en (3) de strategische analyse. Hoe deze vormen van analyse worden gedefinieerd is sterk afhankelijk van de organisatorische context. In een militaire context is de tactische analyse de meest specifieke, op concrete doelwitten gerichte analyse. De term 'operationeel' wordt in deze context gebruikt voor die gevallen waarin een gecombineerde actie tegen vergelijkbare doelwitten wordt verricht, en waarbij onderlinge afstemming en coördinatie noodzakelijk is (zie McDowell 2009: 13-15). Andere organisaties, zoals opsporings- en veiligheidsdiensten, draaien vergeleken met de militaire definities de tactische en operationele analyses om. De operationele analyse ziet dan op analyses van bepaalde personen of organisaties in het kader van een specifieke operatie. De operationele analyseproducten worden met name gemaakt ten behoeve van besluitvorming in concrete inlichtingenoperaties. De tactische analyse is meeromvattend, en bevat verschillende operationele inlichtingenoperaties. Op het tactische niveau gaat het om de samenhang tussen de verschillende operationele inlichtingenoperaties, en het is daarom abstracter dan de operationele analyse. De strategische analyse is nog meer omvattend dan de operationele en tactische analyse, en is meer gericht op het in kaart brengen van brede trends en ontwikkelingen. De strategische analyseproducten informeren en ondersteunen de beleidsmakers van een veiligheidsdienst, hetgeen abstracter is dan de operationele- en tactische analyses (zie McDowell 2009: 13-17aa). In de praktijk is er doorgaans een druk op analisten om operationele en tactische analyses te produceren ten koste van strategische analyses (Phythian en Gill 2006: 85). Wij sluiten ons aan bij de benadering van de opsporings- en veiligheidsdiensten, en laten de hierboven genoemde militaire benadering verder buiten beschouwing.

Omdat operationele analyses en strategische analyses erg veel van elkaar verschillen, vereisen ze andere capaciteiten van een analist. Over het algemeen zal een strategische analyse lijken op (toegepaste) wetenschap en zijn strategische analisten academisch geschoold. Voor een beter begrip van het analyseproces, staan wij in de volgende subsecties stil bij (A) de raakvlakken van analyse en de wetenschap en bij twee verschillen tussen analyse en wetenschap, te weten (B) de tijdsdruk waaronder de veiligheidsdiensten werken en (C) het politieke discours waar zij zich in begeven.

A: Raakvlakken met wetenschap

Intelligence-analyse heeft veel raakvlakken met de wetenschap: het vormt als het ware een onderdeel van een wetenschappelijk proces (Johnston 2005: 17-21). Een goede analyse begint eigenlijk meestal met het formuleren van een probleemstelling. Dit wordt soms door de klant (of de opdrachtgever) gedaan, en soms door medewerkers van de veiligheidsdienst zelf. Een analist zal de opdracht verfijnen en aanpassen en vervolgens weer met de opdrachtgever bespreken. Een analist zal echter, als het goed is, geen analyses op eigen initiatief verrichten: er moet altijd een concrete opdracht aan de analyse ten grondslag liggen. Anders wordt het intelligence-proces een ongeleid proces en zouden producten opgeleverd kunnen worden waar eigenlijk niemand op zit te wachten. Na een concrete opdracht (een probleemstelling) zal de analist een aantal vragen formuleren die leiden tot het oplossen van een hoofdvraag.

Op deze manier wordt het onderzoek van de analist gericht en afgebakend. Het zal duidelijk zijn dat dit voor operationele analyses gemakkelijker is dan voor strategische analyses. De operationele analyses worden afgebakend door de specifieke operatie, en een opdracht zal bijvoorbeeld inhouden dat er een analyse van een informant wordt gemaakt. Een operationeel analist kan na deze fase direct aan de slag met het selecteren van de relevante inlichtingen en met de concrete analyse. De gegevensverzameling wordt voor deze analist afgebakend door de grenzen van het onderzoek waarin de analyse plaatsvindt. Het gaat om specifieke personen en/of organisaties. De analyse zelf zal over het algemeen zijn gericht op het verduidelijken van verbanden tussen personen en organisaties, en de presentatie van de analyse bevat vaak een tijdslijn of een stromenschema. Voor de strategisch analist ligt het allemaal echter nog wat gecompliceerder.

Strategische analyses zijn veel breder, hetgeen specifieke problemen met zich meebrengt. Zo zijn problemen bij de strategische analyse vaak terug te voeren op de fase van de probleemstelling en de vraagstelling. Het is dan niet duidelijk wat de klant precies wil weten (de analist heeft bijvoorbeeld de eigen vragen niet voorgelegd aan de opdrachtgever ter afstemming) en zijn de vragen veel te breed geformuleerd. Deze fase zal bij de strategische analyse dan ook behoorlijk wat tijd en energie vergen.

Indien een opdracht is verduidelijkt, zal de strategisch analist hypothesen (stellingen/claims) opstellen. Deze hypothesen sturen zijn onderzoek, maar kunnen natuurlijk ook worden gefalsificeerd. In de wetenschappelijke onderzoeksmethodologie wordt overigens doorgaans vereist dat er geprobeerd wordt om hypothesen te falsifiëren (de Popperiaanse benadering). Over het algemeen geldt dit niet voor de strategische intelligence–analyse: "*In intelligence usage (and in research in all its forms) hypotheses serve a specific and useful function – to prompt the analyst/researcher to explore the hypothesis further, seeking conclusive data that will either refute or confirm the original idea*" (McDowell 2005: 98). Hypothesen binnen de strategische intelligence analyse verschillen dan ook van de wetenschappelijke hypothesen, maar omdat het in het intelligence-jargon gebruikelijk is om over hypothesen te spreken, doen wij dit in dit proefschrift ook.

Na het formuleren van hypothesen stelt een analist een data-verzamelingsplan op. Anders dan bij de operationele analyse zal er bij strategische analyse een uitgedacht data-verzamelingsplan moeten zijn, omdat de analist anders dreigt te verdrinken in de hoeveelheid informatie (Gill en Phythian 2006: 84-85; Hedley 2007a: 215). Bij strategische analyse zal ook informatie uit open bronnen worden gebruikt, iets dat minder vaak gebeurt bij de operationele analyses (zie Steele 2007). Een andere belangrijke overeenkomst met de wetenschap is dat de strategisch analist theoretische modellen gebruikt voor het verklaren van zijn bevindingen. Deze zijn meestal afkomstig uit de wetenschap, zoals theorieën uit de politicologie, de psychologie, de sociologie, de filosofie en andere gerelateerde wetenschappelijke disciplines. Al met al lijkt met name de strategische analyse dus erg op wetenschappelijk onderzoek, maar er zijn ook belangrijke verschillen die intelligence-analyse tot een geheel eigensoortige discipline maken. Een belangrijk verschil met de wetenschap is de bijzonder hoge tijdsdruk bij de veiligheidsdiensten. Dit verschil zullen wij hieronder behandelen.

B: De tijdsdruk bij de veiligheidsdiensten

Het eerste verschil tussen analyse bij de veiligheidsdiensten en de wetenschap is dat in tegenstelling tot de wetenschap veiligheidsdiensten onder een bijzonder grote

tijdsdruk werken (Johnston 2005: 13-14;). Een inlichtingenanalyse kent dan ook een hele sterke deadline, met name indien het operationele analyses betreft. Maar ook strategische analyses zijn aan strikte deadlines gebonden. Analyserapporten met de stempel 'OBE' zijn doorgaans waardeloos voor de veiligheidsdiensten: *overtaken by events*. De analyse is dan te laat om de besluitvorming te dienen, en zal in dat opzicht waardeloos zijn. De tijdsdruk die heerst bij een veiligheidsdienst is misschien nog wel het beste te vergelijken met de tijdsdruk die je bij krantenredacties tegenkomt. Vaak gaat het om actualiteiten, en op het nieuws van vorige week zit eigenlijk niemand meer te wachten. De druk om op tijd te presteren zal in de praktijk leiden tot kwalitatief mindere producten dan wanneer er voldoende tijd was geweest. Het leidt in ieder geval tot een bijzondere druk op de analisten.

C: Het politieke discours

Een tweede verschil met de wetenschap is de doelstelling van de analyse: het is primair gericht op het politieke discours. Wetenschappelijk onderzoek zal met name gericht zijn op het academisch discours: het gaat onder meer om theorievorming en discussies binnen academische disciplines. Analyses bij veiligheidsdiensten worden echter geschreven ten behoeve van besluitvorming en beogen met name het geven van voorwaarschuwingen van mogelijke dreigingen. Ze moeten veel meer zijn toegesneden op de praktijk en praktisch toepasbaar zijn. Op academische discussies zitten de klanten van een dienst vaak niet te wachten, zij willen antwoorden op prangende vragen en oplossingen voor problemen. In analyserapporten zullen gebruikte theorieën vaak summier worden weergegeven, en de bevindingen behoeven minder empirisch bewezen te worden dan in de wetenschap gewoon is. Zoals al eerder is gezegd, is het werk van de veiligheidsdiensten in grote mate giswerk omtrent wat de toekomst zal brengen. Dit brengt noodzakelijkerwijs onzekerheid met zich mee, onzekerheden en giswerk waarmee de wetenschapper niet weg zal komen. Omdat het publiek waar de analist voor schrijft over het algemeen niet zit te wachten op hele uitgebreide rapportages, zal het uiteindelijke rapport alleen het hoogst noodzakelijke bevatten. In dat opzicht lijken intelligence-analyses summier vergeleken met wetenschappelijke publicaties, maar zij hebben een ander doel.

Omdat (met name strategische) analyses lijken op wetenschappelijk onderzoek, is niet iedereen geschikt om strategische analyses uit te voeren. Meestal worden voor deze functies academici of mensen met uitgebreide onderzoekservaring aangetrokken, zoals journalisten. Het profiel van de analist en de aard van diens werkzaamheden maken de analyseafdelingen in sommige gevallen een beetje een vreemde eend in de inlichtingenbijt. Het is immers bureauwerk en het staat ver van het operationele werk af (Johnston 2005).

Verspreiden

De intelligence-producten moeten uiteindelijk bij de juiste klant terecht komen. Waar een intelligence-product naar verspreid kan worden, hangt af van het soort intelligence-product. Een operationele analyse zal doorgaans naar een teamleider of andere operationele leidinggevende gaan. Strategische analyses gaan vaak naar de hogere leidinggevenden of naar regeringsfunctionarissen. In sommige gevallen worden bepaalde strategische analyses openbaar gemaakt. Deze zijn ontdaan van operationele informatie, maar geven een algemeen inzicht in een specifiek werkveld van de betreffende dienst. Zo heeft de Nederlandse AIVD recent een analyse omtrent

spionage gepubliceerd.[51] Verder heeft de Amerikaanse CIA een website waar ongeclassificeerd onderzoek wordt gepubliceerd; overigens vaak onderzoek dat al redelijk gedateerd is.[52]

Het bij de behandeling van de fase van verwerking beschreven probleem van *stovepiping* wordt bij de verspreiding van intelligenceproducten zichtbaar. Analyses die zijn gemaakt in het kader van contraspionage en die relevante inzichten bevatten voor terrorismebestrijding komen door de interne afscherming niet bij anderen dan de directe klant terecht. De schotten die tussen de afdelingen (en de organisaties) bestaan, houden de verspreiding van intelligence-producten tegen. In hoeverre dit in de praktijk speelt, hebben wij voor de veiligheidsdiensten echter niet vast kunnen stellen.

Het is zeer waarschijnlijk dat een intelligence-product tot nieuwe inzichten en vragen leidt. Hierna is de cyclus rond en begint het hele proces weer opnieuw.

2.4 Kritiek op de intelligence-cyclus

Het model van de intelligence-cyclus wordt van verschillende kanten bekritiseerd omdat het te eenvoudig is en veel aspecten van de realiteit niet meeneemt (de Valk 2005: 14; Gill en Phythian 2006: 32; Turner 2006: 9).[53] Dit is niet zo vreemd, gezien het feit dat het model met name in de praktijk wordt gebruikt om snel het interne werkproces van een dienst te duiden. Het model is evenwel zodanig vereenvoudigd dat het niet alle elementen van het werk van de veiligheidsdiensten kan verklaren (Hulnick 2007).[54] Daarnaast is het model niet bedoeld of ontwikkeld voor wetenschappelijke analyses. Wetenschappelijke onderzoekers zullen het model derhalve enigszins moeten aanpassen om zo meer relevante en verklarende elementen te kunnen meenemen in een analyse. In het model wordt bijvoorbeeld nergens de context waarbinnen de diensten werken genoemd, terwijl die context wel degelijk relevant is. Ontwikkelingen in de context kunnen immers leiden tot aanpassingen van de werking van het model.[55] Gill and Phythian (2006) voegen daarom een aantal

[51] https://www.aivd.nl/onderwerpen/dossiers/spionage, gezien op 6 juli 2010.

[52] https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/index.html, gezien op 6 juli 2010.

[53] De Valk noemt nog twee andere modellen voor inlichtingenwerk: de intelligence-matrix en de waarschuwingscyclus (*warning cycle*). De eerste is product-georiënteerd en verduidelijkt de relatie tussen politiek en intelligence. Dit model houdt echter geen rekening met de relatie tussen intelligence en de context waarbinnen intelligence wordt toegepast. Het tweede model ziet specifiek op de manier waarop een voorwaarschuwing wordt gegeven en op welke manier hierop kan worden gereageerd. De oorsprong van dit model ligt in de psychologie, en voor intelligence-onderzoek is het niet populair. De intelligence-cyclus blijft het dominante model en zal ook in dit proefschrift centraal staan, zij het dat het wel (door ons) is aangepast.

[54] Sommige kritiek op de intelligence-cyclus is volgens ons wat overtrokken. Zo stelt Wheaton (2011) op zijn intelligence-weblog "*let's kill the intelligence cycle*". Zijn belangrijkste argument tegen het gebruik van het model is dat de theorie van de intelligence-cyclus erg ver van de praktijk van het intelligence-werk staat. De realiteit is veel complexer en wordt niet verklaard met behulp van de intelligence-cyclus (zie ook Hulnick 2007). Geen enkel model zal echter alle aspecten van het intelligence-werk kunnen verklaren. De intelligence-cyclus geeft inzicht in het algemene werkproces van een veiligheidsdienst wat de productie van intelligenceproducten betreft. Wij zullen het concept wel aanpassen voor onze analyse, maar voor een verdere analyse van hoe de verschillende fasen van de intelligence-cyclus in de CIE-praktijk functioneren, gebruiken wij andere theoretische inzichten (zie hoofdstuk zeven).

[55] Twee andere elementen die de kern van het werk van de veiligheidsdiensten raken, maar die niet zijn opgenomen in de (traditionele) intelligence-cyclus, zijn de altijd aanwezige dreiging van contra-inlichtingen en de zogenoemde *covert actions* die op basis van intelligenceproducten worden

elementen toe aan de cyclus. Na de fase van 'verspreiding' voegen zij (7) de fase van beleid toe en ze verbinden deze fase met (8) de impact die het heeft op de buitenwereld. De impact op de omgeving (9) verandert de intelligence- en beleidsomgeving, hetgeen weer gevolgen heeft voor de planning- en opdrachtfase waarmee de cyclus rond is (Gill en Phythian 2006: 4). De toegevoegde waarde van dit model is dat de externe omgeving (de context) van de veiligheidsdienst wordt betrokken bij de analyse van het intelligence-concept; zowel de invloed van de omgeving op het intelligence-proces als de invloed van het intelligence-proces op de omgeving worden meegenomen.

Dit is van groot belang voor de verhouding tussen de veiligheidsdiensten en de politie. Voor beide organisaties is de laatste jaren in het kader van terrorismebestrijding veel veranderd, en niet in de laatste plaats daar waar het de (juridische) context betreft. Ontwikkelingen die betrekking hebben op de politie hebben vaak ook invloed op de context van de veiligheidsdienst AIVD en andersom. In Nederland krijgt de politie een steeds grotere rol bij de bestrijding van terrorisme, maar zij krijgt daarnaast ook de verplichting om informatie aan de AIVD te verstrekken.[56] Deze toegenomen aandacht voor terrorisme kan leiden tot nieuwe intelligence-rapporten over dit onderwerp en nieuwe 'bedreigingen' blootleggen, en de nieuwe (verregaande) opsporingsbevoegdheden kunnen een grote impact hebben op de externe omgeving, hetgeen weer nieuwe inzichten oplevert. De (perceptie van de) context verandert en op die manier wordt ook het proces van intelligence beïnvloed.

Alhoewel het model van Gill en Phythian (2006) zeker een stap in de goede richting is, valt ook hier iets op aan te merken. Het probleem van hun model is dat zij aan de relatie tussen de verschillende fasen onzes inziens onvoldoende aandacht besteden. De intelligence-cyclus van Treverton biedt hier weer een oplossing voor (zie Johnston 2005: 49). In zijn visuele weergave van de intelligence-cyclus voegt Treverton eenvoudigweg een aantal verbindingen toe die als dwarsverband tussen verschillende fasen fungeren. Zo geeft hij het bestaan aan van een relatie tussen de analysefase en die van de planning en opdrachten. Hiermee creëert hij in zijn model de mogelijkheid van een cyclus in de bredere cyclus. Wij nemen de aanpassingen van Gill en Phythian en die van Treverton over in ons aangepast model.

2.5 Ons aangepast model

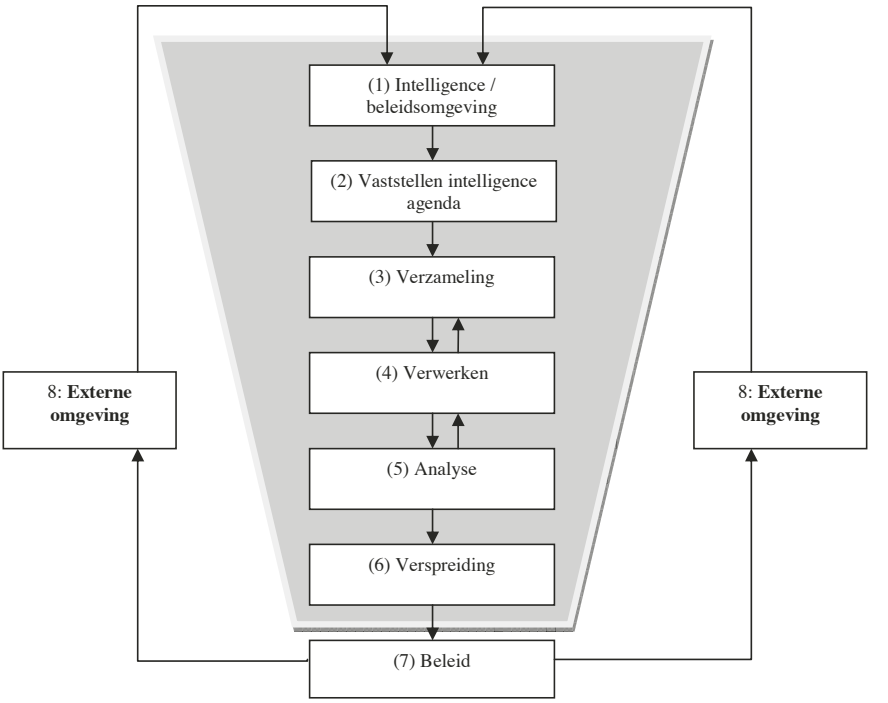
Vanwege de waarde voor de analyse later in dit onderzoek, kiezen wij voor een aangepaste versie van de bovenstaande intelligence-cyclus. De intelligence-cyclus in zijn meest eenvoudige vorm gaat uit van zes kernstappen in het intelligence-concept, stappen die ook in dit onderzoek centraal zullen staan omdat ze een essentieel onderdeel van het werkproces van de veiligheidsdienst zijn: "(...) *there is little argument that there are critical steps in the intelligence process that individually and collectively are designed to fulfil the intelligence mission*" (Turner 2006: 9). Naast het gegeven dat de cyclus praktisch en analytisch goed bruikbaar is, is een andere reden voor het gebruiken van dit model het gegeven dat veiligheidsdiensten zelf aangeven

---

uitgevoerd (Hulnick 2007). Contra-inlichtingen en *covert actions* zijn essentieel voor het moderne intelligencewerk en mogen dan ook niet ontbreken in modellen die (de werking van) intelligence dienen te verklaren.

[56] Zie hoofdstuk drie van dit proefschrift. Zie voor een algemeen overzicht van terrorisme en terrorismebestrijding Muller et al. (2008).

dat de intelligence-cyclus het meest relevante model is.[57] Voor een analyse van de wijze waarop intelligence binnen de politie zou kunnen functioneren, is het daarom logisch om aan te sluiten bij het model dat de diensten zelf ook hanteren. Wij combineren de intelligence-cyclus echter ook met het model van Gill en Phythian en dat van Treverton. Ons model bestaat uit acht elementen waarbij de fasen van verzamelen, verwerken en analyseren onderling verbonden zijn en daarmee een cyclus in de cyclus vormen. Natuurlijk geldt voor dit model ook dat het te eenvoudig is om de complexe werkelijkheid recht te doen, maar het neemt in ieder geval de belangrijkste tekortkoming van de traditionele modellen weg. Ons 8-stappen model is afgebeeld in figuur 2.2.



Figuur 2.2: Het 8-stappen model

2.6 HP-kenmerk 4: geheimhouding

Het vierde kenmerk dat wij behandelen is de geheimhouding. Veiligheidsdiensten en geheimhouding zijn intrinsiek met elkaar verbonden: deze diensten worden niet voor niets ook wel 'geheime diensten' genoemd. In deze sectie behandelen wij drie elementen van geheimhouding. Allereerst bezien wij wat er in het algemeen onder geheimhouding moet worden verstaan (subsectie 2.3.1). Daarna behandelen wij de redenen waarom veiligheidsdiensten geheimhouding betrachten (subsectie 2.3.2). Als laatste behandelen wij de problematische elementen van geheimhouding (subsectie 2.3.3).

[57] Het staat als zodanig genoemd in de CIA *factbook on intelligence.* Zie: www.cia.gov., gezien op 19 april 2009.

2.6.1 Geheimhouding in het algemeen

Geheimhouding is "*anything kept intentionally hidden, set apart in the mind of its keeper as requiring concealment*" (Blank 2009: 64). Het is dus niet hetzelfde als liegen: geheimhouding is een omissie in de zin dat het betekent dat iets wordt nagelaten. Liegen is een opzettelijke misleiding waarbij bewust wordt geprobeerd om anderen te misleiden (Blank 2009: 61). Daarnaast maken wij in dit onderzoek ook een onderscheid tussen privacy en geheimhouding, waarbij wij privacy beschouwen als een recht van een burger op de bescherming van de persoonlijke levenssfeer. Geheimhouding is het opzettelijk (en soms verplicht) achterhouden van informatie en kennis in een organisatorische (overheids)context (zie ook: Shils 2009: 53; Blank 2009: 63). In ons onderzoek bezien we (1) de rol van geheimhouding bij de implementatie van IGP (het intra-organisatorische perspectief) en (2) de rol van geheimhouding in de relatie tussen de CIE en de AIVD (het inter-organisatorische perspectief). Privacy-vraagstukken die zijn gericht op de relatie tussen de overheid en de burger laten wij verder buiten beschouwing.[58]

2.6.2 Redenen voor geheimhouding

Er zijn verschillende redenen voor geheimhouding die sterk afhankelijk zijn van de benadering. *Grosso modo* kan er een onderscheid worden aangebracht tussen (1) de institutionele benadering en (2) de sociale benadering van geheimhouding (Blank 2009). De institutionele benadering ziet geheimhouding als een instrument binnen instituties en organisaties, zoals de bureaucratie (zie Weber 1920; Blank 2009; Shils 2009). De sociale benadering onderzoekt de rol van geheimhouding in sociale relaties tussen verschillende partijen (zie Simmel 1908; Blank 2009). Beide benaderingen gaan uit van verschillende redenen voor geheimhouding welke wij verderop in deze subsectie zullen behandelen. Overigens gaan de in deze subsectie genoemde redenen voor geheimhouding ook op voor geheimhouding door andere overheidsorganisaties, zoals de politie (en dus ook de CIE).

Aftergood (2009: 296-297) noemt naast de bureaucratische geheimhouding ook nog (3) de geheimhouding vanwege de bescherming van de nationale veiligheid (de operationele benadering van geheimhouding) en (4) de politieke geheimhouding.[59] Als we deze benaderingen combineren, komen wij tot drie redenen voor geheimhouding die we in deze subsectie zullen behandelen: (A) de redenen die voortvloeien uit de institutionele benadering, (B) de redenen die voortvloeien uit de sociale benadering en (C) de redenen die voortvloeien uit de operationele benadering. De politieke geheimhouding laten wij verder buiten beschouwing omdat deze niet relevant is in het kader van ons onderzoek.

[58] Wij zullen in hoofdstuk drie, vier en vijf wel ingaan op dataprotectie-regelgeving met betrekking tot de AIVD en de CIE, een aspect van privacy. Deze regelgeving is bedoeld voor de bescherming van de privacy van de burger, maar speelt ook een belangrijke rol bij de implementatie van IGP en de verhouding tussen de CIE en de AIVD.

[59] Volgens Aftergood is politieke geheimhouding: "*the deliberate and conscious abuse of classification authority for political advantage, irrespective of any threat to national security*" (Aftergood 1999: 298).

A: De redenen die voortvloeien uit de institutionele benadering

De institutionele benadering van geheimhouding ziet met name op geheimhouding in relatie tot bureaucratische organisaties. Deze bureaucratische benadering van geheimhouding is in de literatuur verreweg dominant ten opzichte van de andere benaderingen. De grondlegger voor deze bureaucratische geheimhouding is Max Weber (1920).

Volgens Max Weber is de officiële geheimhouding een uitvinding van bureaucratieën en eigen aan het bureaucratische systeem (Weber 1920: 47). De bureaucraat is bij uitstek gespecialiseerd in het reilen en zeilen van het onderdeel van het bestuur waar hij deel van uitmaakt; hij kent het bureaucratische systeem van binnen en van buiten. Geheimhouding en macht zijn volgens Weber met elkaar verbonden (Blank 2009: 60). Vanwege diens superieure specialistische kennis bekleedt de bureaucraat een machtige positie binnen iedere democratie. Dit maakt de formele machthebbers volgens Weber weer afhankelijk en in bepaalde opzichten zelfs ondergeschikt aan de bureaucraat. De bureaucraat zal deze officiële geheimen fanatiek verdedigen tegen alle 'aanvallen' van buitenaf (Weber 1920: 47-48). De beste verdediging is afscherming en geheimhouding. Bureaucratische geheimhouding komt dus met name voort uit concurrentieoverwegingen en speelt in dit opzicht altijd een essentiële rol in de verhoudingen tussen verschillende bureaucratieën. Webers belangrijkste reden voor geheimhouding die voortvloeit uit de institutionele benadering is aldus concurrentie.

Een meer omvattende omschrijving van de redenen van geheimhouding die voortvloeien uit de institutionele benadering wordt gegeven door Sales (2010). Zoals gezegd is geheimhouding verbonden met kennis- en informatieoverdracht. Geheimhouding betekent dat één partij kennis en informatie achterhoudt voor een andere partij. Sales vraagt zich af waarom inlichtingen- en veiligheidsdiensten weigeren om onderling informatie te delen. Hij noemt drie redenen. Volgens Sales ondermijnt het delen van informatie met andere inlichtingen- en veiligheidsdiensten ten eerste de invloed van een dienst over beleidsmakers (2010: 306-310). Dit is het *free-rider* probleem: de andere dienst maakt kosteloos gebruik van de gedeelde informatie en kan zijn zienswijze overbrengen op de beleidsmaker. Ten tweede tast het delen van informatie de autonomie van de inlichtingen- en veiligheidsdienst aan (Sales 2010: 310-313). Het gaat hier om het probleem van de *turf-war*. Vaak concurreren inlichtingen- en veiligheidsdiensten met andere organisaties, en het delen van informatie kan de concurrentie een concurrentievoordeel opleveren. Ten derde is er volgens Sales een culturele belemmering tot het delen van informatie (2010: 323). De interne cultuur van de inlichtingen- en veiligheidsdienst is risico-avers: het delen van informatie levert een risico op voor de betreffende medewerker. Dit verdient een nadere uitleg. De kosten van het delen van informatie wanneer er iets fout gaat wegen voor de individuele medewerker niet op tegen de baten van succesvol delen. We hebben hierboven deze kosten van het delen van informatie reeds beschreven: het verlies van invloed over beleidsmakers en een aantasting van de autonomie. Dit kan de individuele medewerker op een sanctie komen te staan: in het ergste geval ontslag (Sales 2010: 328). Indien informatie succesvol wordt gedeeld (we laten hier de kwalificatie van wanneer het delen van informatie succesvol is buiten beschouwing), zijn de baten voor de individuele medewerker minimaal. Het leidt doorgaans in ieder geval niet tot promotie of verhoging van het salaris (Sales 2010: 328). Al met al hebben de inlichtingen- en veiligheidsdiensten volgens Sales dus weinig redenen om

informatie met andere diensten te delen en des te meer redenen om informatie achter te houden (hetgeen neerkomt op geheimhouding).

B: De redenen die voortvloeien uit de sociale benadering

De sociale benadering van geheimhouding is voor het eerst door de socioloog Georg Simmel beschreven (1908). Hij beziet geheimhouding met name vanuit het perspectief van sociale relaties tussen individuen onderling en individuen en de gemeenschap waar zij deel van uitmaken (Blank 2009: 60). Voor Simmel vormen alles wat bekend is (publiciteit) en alles wat niet bekend is (geheim) de basis voor vrijwel alle sociale relaties (Simmel 1908: 13; Blank 2009: 66). Simmel stelt dat geheimhouding essentieel is voor de relatie tussen mensen en groepen: "*every relationship between two individuals or two groups will be characterized by the ratio of secrecy that is involved in it*" (Simmel 1908: 21). Verder behandelt Simmel geheime genootschappen en stelt dat het hebben van een geheim voor deze organisaties belangrijker is dan het geheim zelf. De inhoud van het geheim is ondergeschikt aan de vorm van het geheim, en vaak blijkt het geheim inhoudelijk irrelevant (Simmel 1908).

Geheimhouding is nauw verbonden met vertrouwen. Vertrouwen is een hypothese omtrent toekomstig gedrag (Hardin 2006; zie ook sectie 8.6) en daarmee zweeft het volgens Simmel tussen een volledige kennis omtrent de ander en een volledig gebrek aan die kennis: "*the possession of full knowledge does away with the need for trusting, while complete absence of knowledge makes trust evidently impossible.*" (Simmel 2009: 13).[60] Of je iemand vertrouwt, hangt dus af van de kennis die je hebt omtrent die ander. Dit betekent dat een zekere transparantie van beide partijen nodig is om de relevante kennis ten behoeve van de betrouwbaarheid te verkrijgen. Vertrouwen is essentieel voor het kunnen uitwisselen van informatie: indien een medewerker van een veiligheidsdienst de medewerker van een andere dienst (zoals de CIE) niet vertrouwt, of andersom, dan zal hij niet snel geneigd zijn om informatie te delen. De vraag is in hoeverre er in de wereld van de veiligheidsdiensten ruimte is voor vertrouwen. Zie voor een uitwerking van het concept van vertrouwen verder hoofdstuk acht.

De redenen van geheimhouding die voortvloeien uit de sociale benadering zijn gelegen in de (complexe) sociale relaties en verhoudingen binnen groepen. Geheimen kunnen een status verlenen aan de geheimhouder en spelen in dat opzicht een rol in de manier waarop iemand in sociale relaties een positief beeld van zichzelf probeert te creëren (zie ook Bartell en Dutton 2001: 120-124). Dit wordt ook wel *impression management* genoemd.

De sociale benadering is voor ons onderzoek erg relevant omdat dit samen met de hierboven beschreven risico-averse cultuur voor een belangrijk deel een verklaring biedt voor de zogenoemde *need to know*-cultuur binnen veiligheidsdiensten (en ook de politiële inlichtingendiensten).

C: De redenen die voortvloeien uit de operationele benadering

De derde benadering van geheimhouding wordt vaak aangehaald door veiligheidsdiensten zelf. Het gaat dan om (1) effectiviteit en (2) veiligheid. Deze twee

[60] Simmel wijkt hiermee overigens af van Hardin: volgens Hardin is de mate van vertrouwen afhankelijk van de mate van kennis, en veel kennis betekent veel of weinig vertrouwen.

redenen voor geheimhouding die voortvloeien uit deze benadering noemen wij 'de operationele redenen voor geheimhouding'.

Met betrekking tot de eerste operationele reden voor geheimhouding: een veiligheidsdienst is alleen maar effectief indien hij grotendeels in het geheim werkt (Turner 2004: 103-104; Gill en Phythian 2006: 6-7). Om effectief proactief te kunnen werken, moeten de activiteiten van de diensten geheim worden gehouden. Want wat hebben voorwaarschuwingen voor zin als de onderliggende methoden, operaties en informatie publiekelijk bekend zijn? Indien subjecten weten hoe een veiligheidsdienst te werk gaat, kunnen ze hierop anticiperen en de activiteiten van die dienst frustreren. Van goede voorwaarschuwingen is dan helemaal geen sprake, hetgeen leidt tot verminderde effectiviteit van de diensten.

De tweede operationele reden voor geheimhouding is de bescherming van de veiligheid en integriteit van informatiebronnen (personen, instellingen, maar ook databanken). Als bepaalde individuen of organisaties weten dat iemand met een veiligheidsdienst praat, dan is niet zelden het leven van de betreffende informant in gevaar. Een dienst die in de ogen van de buitenwereld 'lek' is, zal weinig informanten aantrekken. Ook het feit dat informatie uit open bronnen afkomstig is, dient geheim te blijven. Data uit grote databanken kan namelijk worden gemanipuleerd op het moment dat het duidelijk is dat veiligheidsdiensten er gebruik van maken. Dit is zowel nadelig voor de diensten als voor de eigenaar van de betreffende databanken. Met onbetrouwbare informatie kom je immers ook tot onbetrouwbare intelligenceproducten en een vervuilde databank is ook voor de eigenaar onbetrouwbaar. Geheimhouding heeft dus een legitieme functie voor een veiligheidsdienst: het is essentieel voor het goed kunnen functioneren van die dienst (de effectiviteit) en het beschermt de bronnen (de veiligheid). Daarnaast vormen deze argumenten ook de formele rechtvaardiging voor de geheimhouding.

Een veel gehoorde rechtvaardiging voor een uitbreiding van geheimhouding is de zogenoemde 'mozaïek theorie' (zie Pozen 2005). Deze theorie gaat ervan uit dat een stukje informatie op zichzelf onschadelijk lijkt, maar gecombineerd met andere informatie weleens een beter beeld zou kunnen geven van staatsgeheimen. Dit is op zichzelf geen onjuiste of onbegrijpelijke stelling, maar het maakt het ook heel gemakkelijk voor de veiligheidsdiensten om de geheimhouding verder door te voeren dan strikt noodzakelijk is. Immers, op basis van de mozaïek-theorie is vrijwel alles een potentieel staatsgeheim (Sales 2007: 820).

2.6.3 Problematische elementen van geheimhouding

Geheimhouding is een problematisch kenmerk van de westerse veiligheidsdiensten: een uitgangspunt van een democratische rechtsstaat is immers zoveel mogelijk transparantie. Geheime diensten verhouden zich slecht tot de openheid die in een democratische rechtsstaat van overheidsinstanties wordt verwacht. Wij behandelen in deze subsectie allereerst (A) de negatieve invloed van geheimhouding op de effectiviteit van de veiligheidsdiensten. Daarna behandelen wij kort (B) de normatieve problemen met betrekking tot geheimhouding.

A: Problemen met betrekking tot effectiviteit en efficiency

De geheimhouding zorgt er voor dat een veiligheidsdienst effectief en efficiënt kan werken (de 1^{e} en 2^{e} reden voor geheimhouding). Het tegenstrijdige van geheimhouding is echter dat het ook de effectiviteit en efficiency kan schaden. Zo is

geheimhouding de belangrijkste reden voor het bestaan van verkokering van de diensten. Vanwege het *need to know* denken worden afdelingen van een dienst vaak van elkaar gescheiden en weten ze niet wat de andere doet (Sheptycki 2004; Sales 2010). De geheimhouding bemoeilijkt daarnaast ook de communicatie naar externe partners. Een dienst kan immers zelden inzicht geven in de eigen informatiepositie en activiteiten. Dit maakt een veiligheidsdienst vaak erg kwetsbaar voor kritiek van buitenaf. Het falen van een veiligheidsdienst wordt doorgaans breed in de media uitgemeten, maar de successen blijven over het algemeen geheim. De door de diensten gehanteerde stelling dat geheimhouding essentieel is om succesvol te kunnen functioneren, geldt daarom niet onverkort en verdient een kritische benadering. Shils gaat zelfs verder dan dat en stelt dat de voordelen van geheimhouding niet opwegen tegen de nadelen (Shils 2009: Blank 2009: 63-64). En wat is eigenlijk 'succes' voor een veiligheidsdienst, en wie beoordeelt of het functioneren van een veiligheidsdienst 'succesvol' is?

B: Normatieve problemen

Naast het bovenstaande praktijkprobleem, brengt geheimhouding ook belangrijke normatieve problemen op juridisch, ethisch en democratisch vlak met zich mee (Gill en Phythian 2006).[61] Dit is de normatieve kant van geheimhouding (Blank 2009: 62-65). Op zichzelf is het al een probleem wanneer er geen transparantie is met betrekking tot de veiligheidsdienst. In een democratie is transparantie van de overheid een belangrijk principe, zeker wanneer het om toezicht en controle op veiligheidsdiensten gaat. De veiligheidsdienst is een onderdeel van de uitvoerende macht, en moet in een democratische rechtstaat worden gecontroleerd door de wetgevende en rechtsprekende machten (de scheiding der machten door middel van *checks and balances*). Zonder transparantie zijn echter geen toezicht en controle mogelijk. De veiligheidsdiensten in een democratische rechtsstaat maken een inbreuk op de rechten van burgers (met name privacy), en zullen daarom gecontroleerd en getoetst moeten worden. Indien een veiligheidsdienst geheimhouding betracht, zegt hij daarmee namelijk eigenlijk dat hij de burger en de rest van de buitenwereld niet vertrouwt. Dit brengt echter ook het beeld met zich mee van de dienst die iets te verbergen heeft, hetgeen funest is voor het vertrouwen van burgers en politiek in de dienst (Shils 2009).[62]

2.7 De politie

Een veiligheidsdienst zal moeten communiceren en samenwerken met andere (overheids)organisaties, hetgeen door de geheimhouding wordt bemoeilijkt. Dit heeft invloed op de relatie met de politie. Maar de geheimhouding gecombineerd met de voorspellende taak van bijvoorbeeld de veiligheidsdienst maakt deze dienst voor de politie bijzonder aantrekkelijk. De politie wenst zelf immers ook proactief te werk te

[61] Turner zegt hierover het volgende: "*secrecy in intelligence comes into conflict with the American democratic tradition of transparancy in government"* (Turner 2006: 103). Zie ook Born en Thorsten (2007).

[62] Veel democratische rechtsstaten hebben ingewikkelde systemen voor toezicht en controle op de activiteiten van de inlichtingen- en veiligheidsdienst in het leven geroepen. Deze systemen verschillen aanzienlijk van elkaar, maar er is wel consensus in de academische literatuur en de politiek over het feit dat het toezicht in ieder geval door een onafhankelijke instantie moet worden uitgevoerd en dat dit zoveel mogelijk openbaar dient te zijn (Commissie Havermans 2004: 200; Gill en Phythian 2006: 148-171).

gaan, en kijkt naar de veiligheidsdiensten om te zien hoe dat kan. Intelligence (en de intelligence-cyclus) bieden de mogelijkheid om dit te bereiken. De politie moet echter van ver komen wil zij intelligence-gestuurd kunnen gaan werken. Een traditionele politiedienst is namelijk het spiegelbeeld van een veiligheidsdienst: zij wordt niet voor niets de lage politie genoemd. In de volgende secties behandelen wij de LP-kenmerken van de traditionele politieorganisatie.

Net als bij de veiligheidsdiensten onderscheiden wij bij de politie ook vier LP-kenmerken, te weten: (1) de handhaving van de rechtsorde, (2) waarheidsvinding, (3) opsporingsonderzoek en (4) transparantie. Deze kenmerken vormen als het ware het spiegelbeeld van de HP-kenmerken van de veiligheidsdienst. Let wel, het gaat hier niet om een gedetailleerde (juridische) analyse van de Nederlandse politie, maar om een meer algemeen beeld van wat de politie in hoofdlijnen doet. Het doel is om kort en kernachtig de verschillen tussen de veiligheidsdienst en de politie aan te stippen. In de volgende secties wordt daarom slechts een algemeen beeld van de politie geschetst, een beeld dat toepasbaar is op vrijwel alle (traditionele) politiediensten.

In hoofdstukken vier en vijf zullen de kenmerken specifiek voor de Nederlandse situatie worden uitgewerkt en gaan wij in op de belangrijke veranderingen die de politie de laatste jaren heeft doorgemaakt. De Nederlandse situatie wordt in dit hoofdstuk slechts gebruikt als voorbeeld. Aan de hand van deze kenmerken beoordelen wij in hoofdstuk acht in hoeverre er nog sprake is van een scheiding tussen de veiligheidsdienst AIVD en de CIE.

2.8 LP-kenmerk 1: handhaving van de rechtsorde

Wat is precies de taak van de politie? Deze vraag is niet zo gemakkelijk te beantwoorden. De visie op de taak en functie van de politie hangt in grote mate af van de sociaal-maatschappelijke context van het politiewerk op een bepaald moment. De samenleving van nu is heel anders dan die van de jaren ‘60 van de vorige eeuw, en dit maakt de politiefunctie bezien door de bril van de jaren ‘60 dan ook heel anders dan die bezien door de bril van 2012. Dit neemt echter niet weg dat er wel een bepaalde rode draad is waar te nemen die weinig verandert. In deze sectie geven wij een korte weergave van de kernfunctie van de politie, waarbij het doel is om het belangrijkste verschil met de veiligheidsdienst te duiden.

Een korte blik op de taakstelling van de Nederlandse politie laat duidelijk zien wat de politie allemaal wordt geacht te doen. Artikel 2 van de Politiewet 1993 formuleert het als volgt: “*De politie heeft tot taak in ondergeschiktheid aan het bevoegde gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven.*” Alhoewel de (strafrechtelijke) handhaving van de rechtsorde (de juridische term voor de opsporing van strafbare feiten, oftewel criminaliteitsbestrijding) de focus is van dit onderzoek, is dit niet (in kwantitatieve zin) de hoofdactiviteit van de politie. Een heel groot deel van het politiewerk bestaat uit verkeerscontroles, optreden tegen overlast en andere zaken die van doen hebben met de handhaving van de openbare orde of de hulpverlening. Dit blijkt ook uit buitenlands onderzoek: verreweg de belangrijkste politieactiviteit is surveillance (in de zin van *patrolling,* zie Baley 1994: 141-144). De volgende belangrijkste

politieactiviteit is wel de opsporing van strafbare feiten, waarover in sectie 2.11 meer.[63]

Een belangrijk aspect van deze centrale taak van de politie is dat de politie niet vaststelt welke regels tot de rechtsorde behoren en welke niet. Dit is een taak van de wetgevende macht. De politie heeft geen discretionaire ruimte om te besluiten dat bepaalde soorten gedragingen strafbaar zouden moeten zijn en dus vallen onder de centrale taak van de strafrechtelijke handhaving van de rechtsorde. Ze kan slechts concrete gedragingen aan bestaande, door de wetgever geformuleerde strafrechtelijke normen toetsen. In dit opzicht wijzen wij voor de Nederlandse situatie op het strafrechtelijk legaliteitsbeginsel van artikel 1 WvSr: "*Geen feit is strafbaar dan uit kracht van een daaraan voorafgegane wettelijke strafbepaling.*"[64] Indien een gedraging niet strafbaar is, dan valt deze niet onder de hierboven geformuleerde centrale taak van de handhaving van de rechtsorde. Hier zit een essentieel verschil met de veiligheidsdiensten, omdat deze diensten een zeer grote discretionaire ruimte hebben bij de beoordeling welke gedragingen wel en welke gedragingen geen bedreiging van de nationale veiligheid vormen. Er zijn geen wettelijke bepalingen waarin wordt aangegeven welke normen onder de noemer 'nationale veiligheid' vallen.

Overigens betekent het bovenstaande niet dat de politie een a-politieke organisatie is. De strafbaarstelling van bepaalde handelingen is op zichzelf een politieke aangelegenheid: criminaliteit en strafrecht zijn politiek (zie Garland 2002; Simon 2007; Findlay 2008; Van der Woude 2010). Via het strafrecht worden bepaalde heersende opvattingen over normen en waarden geregeld, zaken die verband houden met bepaalde levensbeschouwelijke (politieke) opvattingen. Het strafrecht kan ook instrumenteel zijn in het uitvoeren van strafrechtelijk beleid, hetgeen een exponent van de politiek is (Simon 2007). Dit betekent dat de politie zelf altijd een politieke functie heeft. Het grote verschil met de veiligheidsdienst is echter dat de veiligheidsdienst zich specifiek richt op het beschermen van het politieke systeem. Het is zijn belangrijkste taak. Voor de politie is het politieke element van het werk veel meer een afgeleide van het politieke systeem in het algemeen.

Een meer theoretische benadering van het politiewerk komt van Bittner (2005). Hij stelt dat de primaire taak van de politie bestaat uit het oplossen van conflictsituaties: "(...) *police are empowered and required to impose, or, as the case may be, coerce a provisional solution upon emergent problems without having to brook or defer to opposition of any kind, and that further, their competence to intervene extends to every kind of emergency, without any exceptions whatever*" (Bittner 2005: 150). De politie moet volgens Bittner dus met name problemen oplossen en heeft hiertoe een machtig middel gekregen, te weten geweld. Bittner constateert dat er een verschil is tussen de vermeende taak van de politie en de daadwerkelijke taak. Volgens hem voedt de politie dit beeld zelf ook. Zo wordt binnen de politieorganisatie vaak het beeld van de politieman als *crimefighter* neergezet. De primaire taak van de politie is dan 'boeven-vangen'. Ook de interne bureaucratische organisatie van de politie lijkt het beeld van de boevenvanger te propageren (Bittner 2005). De opleiding van politiemensen legt een bijzondere nadruk op criminaliteit en strafrecht. Daarnaast ziet de politiële informatiehuishouding

[63] De omvang van de politietaak zorgt ervoor dat de politie ook een bijzonder grote organisatie is. Zo telt het grootste politiekorps Amsterdam-Amstelland meer dan 6.000 medewerkers, en het kleinste korps Gooi- en Vechtstreek 700 medewerkers. In totaal werken er ongeveer 50.000 mensen bij de 26 Nederlandse politiekorpsen.

[64] Dit beginsel is ook opgenomen in artikel 16 van de Grondwet.

volgens Bittner met name op de handhaving van de strafrechtelijke rechtsorde (Bittner 2005: 153-154). Als iemand binnen de politie carrière wil maken, wordt met name gekeken naar de staat van dienst op het gebied van de strafrechtelijke handhaving van de rechtsorde, en in veel mindere mate naar de hulpverlening. Het (correct toepassen van het) strafrecht is bovendien vaak ondergeschikt aan de pragmatische en probleemoplossende vaardigheden van de politieman. Dit kenmerk zou, gecombineerd met de carrièreperspectieven van de gemiddelde politieman en de status van de criminaliteitsbestrijding, weleens van grote invloed kunnen zijn op de wijze waarop IGP in de praktijk vorm krijgt, zo vooronderstellen wij voorshands.

De taak van de politie omvat dus meer dan het bestrijden van criminaliteit. In dit onderzoek gaat het echter om de bestrijding van terrorisme en georganiseerde criminaliteit. We beperken ons dan ook tot kenmerken die van belang zijn voor deze twee specifieke aandachtsgebieden van het politiewerk. Bij de strafrechtelijke handhaving van de rechtsorde richt de politie zich op datgene wat feitelijk is gebeurd. De dwangmiddelen waarmee de politie een inbreuk maakt op de rechten van individuen mogen niet zomaar worden toegepast: zij worden toegepast in het kader van de waarheidsvinding. Met andere woorden: de politie onderzoekt wat er daadwerkelijk is gebeurd, voor zover dit strafrechtelijk relevant is. Dit is het onderwerp van de volgende sectie.

2.9 LP-kenmerk 2: de strafprocesrechtelijke waarheidsvinding

In het kader van de opsporing van strafbare feiten doet de politie aan strafprocesrechtelijke waarheidsvinding (Jörg en Kelk 2001: 192 e.v.; Myjer 2002; Corstens 2008: 371). Op zichzelf biedt de term 'waarheidsvinding' voldoende aanleiding voor uitgebreide juridische en zelfs filosofische beschouwingen over wat 'waarheid' precies is, en of het strafrecht de aangewezen manier is om waarheidsvinding te betrachten (zie De Vries 2002; Crijns, Van der Meij en Ten Voorde 2008). Dit onderzoek is daar niet de plaats voor. Wij beschouwen de strafprocesrechtelijke waarheidsvinding in het opsporingsonderzoek eenvoudigweg als het onderzoek verricht door de politie naar wat er feitelijk is gebeurd met betrekking tot één of meer vermoedelijk begane strafbare feiten. Hieruit volgt een element van de strafprocesrechtelijke waarheidsvinding dat voor dit onderzoek wel relevant is: het is per definitie een activiteit die is gericht op het verleden. Het gaat erom vast te stellen wat er is gebeurd. Een traditionele politiezaak begint dan ook over het algemeen met een verdenking van een concreet gepleegd misdrijf. Vanaf dat moment komt de politie in actie en probeert zij helder te krijgen wat er precies is gebeurd, wie erbij betrokken zijn, waarom het misdrijf heeft plaatsgevonden *et cetera*. De politie richt zich hierbij dus op het verleden, op wat er precies is gebeurd, en niet op wat er mogelijk in de toekomst nog te gebeuren staat. Met andere woorden, traditioneel politiewerk is reactief in de zin dat de politie zich 'aanvankelijk afwachtend opstelt' (Corstens 2008: 269). Reactief politieoptreden wordt dan ook veelal geïnstigeerd door de burger (Ericson 2005: 228). Hier ligt een belangrijk verschil met de veiligheidsdienst, die juist proactief is en zich op toekomstige bedreigingen van de nationale veiligheid richt (HP-kenmerk 1).

De strafprocesrechtelijke waarheidsvinding door de politie richt zich niet op alle aspecten van wat er is gebeurd, slechts op datgene wat relevant is voor (de latere beoordeling door de rechter van) het gepleegde misdrijf. In het strafrecht wordt de complexiteit van de werkelijkheid dus gereduceerd tot juridisch (strafrechtelijk) relevante proporties (Van de Bunt 2002; Corstens 2008: 558). In dat opzicht is het

werk van de politie behoorlijk afgebakend: slechts de strafrechtelijk relevante waarheid is van belang. Het werk van de politie is in dit opzicht daardoor veel meer ingekaderd tot specifieke gebeurtenissen dan dat van de veiligheidsdienst.

Het doel van het gehele strafrecht is het ontdekken van de materiële waarheid, en de politie heeft daarin een belangrijke rol (Jörg en Kelk 2001: 192; Corstens 2008: 331). Het gaat niet om de subjectieve waarheid, de belevenis van een specifieke politieman omtrent wat er gebeurd moet zijn, maar het gaat om de objectieve, door feiten gestaafde waarheid. Op basis van het werk van de politie wordt er dikwijls een inbreuk op de rechten van een individu gemaakt of kan iemand strafrechtelijk worden veroordeeld, hetgeen vereist dat dit op een zo objectief mogelijke weergave van de werkelijkheid gebeurt. De subjectieve beleving omtrent wat er is gebeurd wordt zoveel mogelijk omgevormd in juridisch relevante kwalificaties, met als doel het bevorderen van een zoveel mogelijk objectieve weergave van hetgeen is gebeurd. De politie heeft in dit opzicht een belangrijke rol, zij is namelijk belast met het verzamelen van zoveel mogelijk feiten die een bepaalde veronderstelling omtrent de strafrechtelijk relevante waarheid bevestigen danwel ontkrachten. Vaak is de politie de eerste die een bepaalde situatie of handeling strafrechtelijk dient te kwalificeren (zij is immers vaak de eerste die een mogelijk strafbaar feit constateert).

Om het werk van de politie en justitie nog verder te compliceren: zij dient niet alleen op basis van feiten en omstandigheden een zo objectief mogelijk beeld van hetgeen is gebeurd te schetsen, de officier van justitie moet op basis van het werk van de politie de rechter (of een jury, dat hangt af van het betreffende juridische systeem) ook nog eens overtuigen van dit beeld. Met andere woorden: de waarheid moet wettig en overtuigend bewezen worden. In dit opzicht is de term waarheidsvinding misschien misplaatst (zie Myjer 2002). Immers, de politie kan wel van mening zijn de waarheid te hebben vastgesteld, maar als de strafrechter niet is overtuigd door de lezing van de politie, zal de concrete zaak niet zijn opgelost. Hiermee is nog niet gezegd dat het door de politie gestelde onwaar is, het betekent slechts dat zij de rechter niet heeft kunnen overtuigen. Overigens moet de politie ook bepaalde procedurele vereisten in acht nemen bij het vaststellen van de strafprocesrechtelijke waarheid. Met andere woorden: de strafprocesrechtelijke waarheidsvinding wordt getemperd door het vereiste van rechtmatig overheidsoptreden (Jörg en Kelk 2001: 193). De vaststelling van de waarheid door de politie waarbij processuele regels zijn geschonden, kan wellicht rekenen op een sanctie van de strafrechter. Dit kan ertoe leiden dat een verdachte wordt vrijgesproken omdat bijvoorbeeld onrechtmatig verkregen bewijs wordt uitgesloten van de bewijsvoering (zie Corstens 2008: 663 e.v.). In de ernstigste gevallen van schendingen van processuele regels door de politie kan de rechter het OM niet ontvankelijk verklaren. Ook hiermee wordt overigens niet direct gezegd dat wat de politie stelt niet waar is, maar wel dat het niet op de juiste manier is vastgesteld. De uitkomst is hetzelfde: de door de politie voorgestelde visie op de werkelijkheid vindt geen steun bij de rechter.

Het werk van de politie is in dit opzicht dan ook veel meer gericht op zekerheid dan het werk van de veiligheidsdienst. De veiligheidsdienst richt zich op de toekomst, iets wat per definitie onzeker is. Met andere woorden, de veiligheidsdienst doet aan geïnformeerd giswerk. De inschattingen van een dergelijke dienst zullen dan ook altijd een bepaalde marge van onzekerheid bevatten, onzekerheden waarmee de traditionele politie over het algemeen niet kan werken. Afhankelijk van de mate van onzekerheid zal dit bij het werk van de politie ervoor zorgen dat een zaak eenvoudigweg niet is opgelost. Dat dit onderscheid vandaag de dag onder druk staat

en mogelijk zelfs niet meer voor de politie opgaat, is het onderwerp van hoofdstukken vijf, zeven en acht.

Zoals gezegd doet deze politie onderzoek naar de materiële, strafrechtelijk relevante waarheid en verzamelt zij hiertoe bewijs omtrent reeds gepleegde strafbare feiten. Dit doet zij door middel van opsporingsonderzoeken, wat ons tot de volgende sectie brengt.

2.10 LP-kenmerk 3: opsporingsonderzoek

De waarheidsvinding door de politie vindt plaats in het kader van het opsporingsonderzoek, hetgeen uiteen valt in twee fasen. Indien er een misdrijf is gepleegd, zal de politie hierop reageren door enerzijds het verhaal van wat zich heeft afgespeeld te reconstrueren (de reconstructiefase) en anderzijds door het zoeken naar informatie waarmee dit verhaal kan worden bewezen (de verificatiefase).[65] Deze fasen lopen door elkaar heen en kunnen in de rechercheprakijk niet los van elkaar worden gezien (De Poot et al. 2004: 46-47).

Er zijn verschillende soorten opsporingsonderzoeken te typeren (De Poot et al. 2004: 50). Allereerst zijn er (1) de zogenoemde 'klip en klaar' onderzoeken. Dit zijn zaken waarbij de politie iemand op heterdaad betrapt, in de buurt van het misdrijf aantreft of iemand geeft zichzelf aan. Deze zaken zijn vrij eenvoudig op te lossen, en de onderzoeksactiviteiten zijn er dan ook op gericht om bewijs te verzamelen tegen de specifieke verdachte(n). Daarnaast zijn er (2) 'verificatiezaken', (3) 'opsporingszaken' en (4) 'zoekzaken'.

Verificatiezaken zijn opsporingsonderzoeken waarbij al vanaf het begin duidelijk is wat er is gebeurd en wie er (mogelijk) als verdachte(n) bij betrokken is (zijn). De politie zal zich hierbij met name richten op het verifiëren van het verhaal en ook hier geldt dat het verzamelen van bewijs de kernactiviteit van de politie is.[66] Het verschil met de klip en klaar onderzoeken is dat bij verificatieonderzoeken een betrokkene anders dan de verdachte het verhaal bij de politie aanbrengt. Dit is bijvoorbeeld het geval wanneer een slachtoffer aangifte doet en daarbij ook een verdachte noemt (De Poot et al. 2004: 50).

Bij opsporingszaken zal de politie nog een verdachte bij het verhaal op dienen te sporen. Hier is niet zozeer de verificatie van het verhaal door middel van het verzamelen van bewijs het belangrijkste, maar zal de nadruk liggen op het identificeren van een verdachte. Wat overigens niet betekent dat er geen bewijs wordt verzameld. Vaak kan bepaald bewijsmateriaal al worden verzameld en veilig worden gesteld, waarbij het niet altijd duidelijk is welke informatie in een later stadium precies als bewijs kan gaan dienen. Die beoordeling kun je pas maken als er een concrete verdachte in beeld is.

Het lastigst zijn de zoekzaken. Hierbij is niet duidelijk wat er precies is gebeurd en wie erbij betrokken zijn. De politie zal zowel een verhaal over wat er heeft

[65] De Poot et al. (2004: 47) spreken van 'hypothetico-deductief redeneren': gedurende het onderzoek wordt het verhaal verder geconstrueerd, getoetst, bekritiseerd en aangepast om zo dichtbij een het waargebeurde verhaal te komen. Wij merken hierbij op dat de hypothetico-deductieve methode, zoals deze in de wetenschap wordt gehanteerd, met name uitgaat van het falsificeren van hypotheses. De politie lijkt echter met name te zijn gericht op het bevestigen van het verhaal (de hypothese). De genoemde auteurs spreken niet voor niets over een verificatiefase, en niet van een falsificatiefase. Zie sectie 2.4 voor een vergelijkbaar verschil tussen intelligence en wetenschappelijke onderzoeksmethoden.

[66] De Poot e.a. (2004) spreken van het reconstrueren van verhalen omtrent strafbare feiten wanneer ze het hebben over de functie van het opsporingsonderzoek.

plaatsgevonden moeten reconstrueren als een verdachte hierbij moeten vinden. Deze zoekzaken vragen van de politie de grootste inspanning. Net als bij de opsporingszaken staat bij dit type onderzoek de identificatie van de verdachte centraal.

De laatste categorie van zaken (5) zijn zaken die in een beginfase de status hebben van 'klip- en klaar' zaak of verificatiezaak, maar die eigenlijk helemaal niet zo klip en klaar of duidelijk zijn. Dit zal met name een risico zijn bij zeer zware misdrijven die een bijzondere inspanning van de politie vereisen, en waarbij eigenlijk al direct een verdachte in beeld is. Hier speelt het risico dat de politie enkel nog maar zoekt naar bewijsmiddelen die de betrokkenheid van de verdachte bevestigen, en informatie die deze betrokkenheid ontkracht wordt dan al snel genegeerd. Dit staat bekend als het 'tunnelvisie' fenomeen. In Nederland is dit fenomeen bekend geworden van zaken als de Schiedammer parkmoord (Commissie Posthumus 2006). Het mag duidelijk zijn dat dergelijke zaken met materiële waarheidsvinding weinig van doen hebben. Dit risico geldt overigens voor alle typen opsporingsonderzoek. Waar dit risico precies vandaan komt wordt duidelijk als het opsporingsonderzoek wat nader wordt bekeken.

Op een gegeven moment zal er in een opsporingsonderzoek sprake zijn van een verdenking omtrent wie het strafbare feit gedaan zou kunnen hebben. Vervolgens wordt er gezocht naar informatie die deze verdenking bevestigt en een aanhouding en vervolging mogelijk maakt (Baley 1994: 145; Gill 2008; Ratcliffe 2008). Dit is de verificatiefase waarin de politie naar bewijsmiddelen zoekt voor het door hen geconstrueerde verhaal.[67] Het verzamelen van het bewijs kan op verschillende manieren plaatsvinden. Zo kunnen verregaande (heimelijke) opsporingsmethoden worden toegepast, zoals een telefoontap, een inkijk-operatie, maar ook het verhoor van getuigen en verdachten. Deze opsporingsmethoden worden ook wel dwangmiddelen genoemd. Omdat de toepassing van dergelijke dwangmiddelen, het woord zegt het eigenlijk al, dwang inhouden en er dus een inbreuk wordt gemaakt op de rechten van een burger, gelden er vaak procedures die gevolgd moeten worden en strenge criteria waaraan moet worden voldaan (Jörg en Kelk 2001). Er zal vrijwel altijd sprake moeten zijn van een verdachte tegen wie het dwangmiddel wordt ingezet. Maar voordat iemand als verdachte kan worden aangemerkt, zal de politie aan een aantal (vrij strikte) criteria moeten voldoen. In Nederland volgt dit uit artikel 27 Wetboek van Strafvordering: een verdachte is iemand ten aanzien van wie uit feiten en omstandigheden een redelijk vermoeden van schuld aan enig strafbaar feit volgt. Er zijn dus feiten en omstandigheden nodig, en het vermoeden moet redelijk zijn. Overigens stelt het artikel ook iets dat voor de vorige sectie van belang is: er moet sprake zijn van een strafbaar feit. Het plegen van niet-strafbare feiten legitimeert niet de toepassing van dwangmiddelen door de politie. Deze criteria gelden niet alleen in Nederland, ook elders in de wereld kom je vergelijkbare eisen tegen. Zo moet er voordat er in de V.S. een inbreuk gemaakt kan worden op de rechten van een Amerikaans staatsburger eerst sprake zijn van een '*reasonable suspicion*'. Dus niet alleen de waarheidsvinding is ingekaderd door het strafrecht (het gaat immers om de

[67] Wat er in juridisch opzicht precies onder 'bewijs' moet worden verstaan, verschilt van land tot land. Het past niet in dit onderzoek om hier op in te gaan. Wij laten in dit onderzoek het Nederlandse bewijsrecht verder grotendeels dan ook buiten beschouwing.

juridisch relevante waarheid), ook de wijze waarop de politie de waarheid tracht te achterhalen is gebonden aan wettelijke bepalingen.[68]

In een opsporingsonderzoek gaat het er dus erg verschillend aan toe vergeleken met een onderzoek van een veiligheidsdienst. De rechercheurs hebben bijzonder veel vrijheid en doen traditioneel vanaf het begin van een onderzoek het meeste werk zelf. Zo formuleren zij de veronderstellingen, passen zij de opsporingsmethoden toe, analyseren informatie, construeren een verhaal *et cetera.* Dat is een groot verschil met de veiligheidsdienst, die veel meer weg heeft van een beleidsorganisatie. Daar is het proces veel meer onderverdeeld in verschillende fases, met elk een eigen expert. Het verzamelen van informatie wordt daar door mensen gedaan die dat als een specifieke taak hebben (zoals de operateurs, zie hoofdstuk drie), en voor de analyse gebruikt de veiligheidsdienst de analist. Dat de politie tegenwoordig steeds meer gebruik maakt van bijvoorbeeld analisten, is iets van de laatste tijd en komt onder meer door de implementatie van IGP (zie hoofdstuk vijf).

Een belangrijk kenmerk van het opsporingsonderzoek is ook dat de dwangmiddelen worden toegepast met als doel het handhaven van de rechtsorde. Het gaat primair om het verkrijgen van relevante informatie (bewijs). In de praktijk betekent dit dat informatievergaring door de politie plaatsvindt met het oog op het verzamelen van bewijs, en dus niet om het verkrijgen van een algemene informatiepositie in de samenleving. Dit is één van de belangrijkste verschillen met een veiligheidsdienst, die feitelijk als belangrijkste taak heeft het opbouwen en in stand houden van een informatiepositie (HP-kenmerk 2). Dat de politie wel degelijk een bijzonder goede informatiepositie heeft of kan hebben, is het gevolg van haar unieke positie in de samenleving en een bijkomend gevolg van de toepassing van dwangmiddelen, maar het mag niet het primaire doel zijn van die toepassing. De enige informatiepositie waarvoor dit wel is toegestaan, is die van het bewijs in een concrete strafzaak. Vanwege de ontwikkeling en implementatie van IGP, waarbij een nadruk komt te liggen op criminaliteitsanalyse en de informatiepositie van de politie, komt dit uitgangspunt onder druk te staan.

Omdat de politie met de toepassing van dwangmiddelen een inbreuk maakt op de rechten van een burger, is deze toepassing onderworpen aan diverse vormen van toetsing en controle. Om de toetsing en controle goed uit te kunnen voeren, zal het handelen van de politie voldoende transparant moeten zijn. De noodzaak van transparantie is het onderwerp van de volgende sectie.

2.11 LP-kenmerk 4: transparantie

De politie is de instantie die binnen de grenzen van de rechtsstaat gebruik mag maken van geweld jegens burgers. Om die reden moet het optreden van de politie altijd transparant zijn.[69] Dit betekent niet dat er bij de politie geen ruimte is voor geheimhouding, maar deze geheimhouding dient een uitzondering te zijn en is in ieder geval tijdelijk van aard. Uiteindelijk moet de politie aan de strafrechter een volledige openheid van zaken geven omtrent hetgeen zij allemaal heeft gedaan in een specifiek opsporingsonderzoek. Dit betekent dan ook dat de rechercheur veel van zijn handelingen schriftelijk moet vastleggen. Zo moeten in Nederland alle

[68] De politie kan de waarheidsvinding niet ten koste van alles uitvoeren. Deze gebondenheid aan procedures doet sommigen concluderen dat de strafrechtelijke reductie van de werkelijkheid ten koste gaat van de waarheidsvinding (Van de Bunt 2002).

[69] Zie voor een behandeling van de noodzaak voor transparantie in de Nederlandse opsporing: Beijer et al. (2004).

opsporingshandelingen worden geverbaliseerd in een proces-verbaal (artikel 152 Wetboek van Strafvordering). Het proces-verbaal wordt aan het onderzoeksdossier toegevoegd. De door de opsporingsambtenaren verrichte handelingen worden dus, als vertrekpunt, vastgelegd zodat ze later door een strafrechter kunnen worden getoetst. Niet naleving van dit voorschrift kan leiden tot de niet-ontvankelijkheid van het OM. Deze verplichting van politiediensten om alles te verbaliseren is ook wel de 'tirannieke werking van het (politiële) onderzoeksdossier' genoemd: vrijwel alle handelingen van de politie worden vastgelegd zodat deze in een later stadium kunnen worden gecontroleerd (Shelby 2002: 62).[70] Er zijn in principe geen mogelijkheden om bepaalde informatie buiten het dossier te houden, behoudens bepaalde specifieke details die, wanneer bekend, een direct levensgevaar voor betrokkenen kunnen opleveren. Geheimhouding bij de politie is hiermee dus een uitzondering, in tegenstelling tot de situatie bij de veiligheidsdienst. Deze transparantie geldt overigens voor het gehele strafproces, en staat in Nederland bekend als het principe van de interne openbaarheid voor wat betreft de direct bij het strafproces betrokkenen die vanuit hun rol aanspraak maken op de toegang tot verhoren of inzage in de stukken. Het gaat dan concreet om de verdachte(n) en diens raadsman. De algemene openbaarheid van het strafproces voor een ieder staat bekend als het principe van externe openbaarheid (zie Van Lent 2008: 1).

Betekent de noodzaak voor transparantie automatisch dat de politie geen geheimhouding kent? Nee, verre van dat. Ook de politie, en dan met name de opsporingseenheden, kennen vormen van geheimhouding, en soms gaat deze geheimhouding bijna net zo ver als bij de veiligheidsdiensten. Tot op zekere hoogte heeft dit te maken met legitieme redenen, zoals de noodzaak tot afscherming van de identiteit van getuigen en informanten of een eventueel afbreukrisico van opsporingsonderzoeken indien informatie bekend wordt bij de verdachte(n). Deze geheimhouding is echter formeel beperkt tot hetgeen strikt noodzakelijk is. Het zijn de uitzonderingen op de hoofdregel van transparantie. Daarnaast zal een rechter, als hij dat echt noodzakelijk acht, de geheimhouding kunnen doorbreken. Zo zijn in Nederland de CIE-en belast met het onderhouden van contacten met informanten, en doorgaans wordt de identiteit van de informant ook afgeschermd voor de strafrechter. Maar het is aan de rechter zelf om te bepalen of de geheimhouding noodzakelijk is en blijft (zie Van der Bel et al. 2009: 208 e.v.). Mocht de rechter oordelen dat andere belangen zwaarder wegen dan de geheimhouding van de identiteit van de informant, dan kan hij bepalen dat de informant gehoord dient te worden. Op deze manier kan de geheimhouding worden doorbroken.

Naast de legitieme redenen voor geheimhouding zijn de meer culturele redenen van belang. Ook binnen de politie geldt kennis is macht, en dit ligt aan de basis van veel geheimhouding (zie Manning 2005: 208-209; zie ook sectie 2.7). Deze aspecten van geheimhouding worden verder besproken in hoofdstuk zeven en acht.

2.12 Hoofdstukconclusie: antwoord OV 1

OV 1 luidt: *Wat zijn de traditionele kenmerken van veiligheidsdiensten en de politie?* Van de veiligheidsdiensten en de politie hebben we in dit hoofdstuk de belangrijkste kenmerken gegeven en deze kenmerken vormen als het ware een spiegelbeeld. De

[70] Shelby (2004) ziet de tirannieke werking van het procesdossier als een aspect van de FBI-cultuur die de FBI tot een slechte intelligence-organisatie maakt. Hij schreef over de verbeteringen die volgens hem na de aanslagen van 11 september 2001 in de Amerikaanse intelligence-gemeenschap doorgevoerd moesten worden.

kenmerken worden later in het proefschrift gebruikt om te beoordelen in hoeverre IGP leidt tot een vermenging van de veiligheidsdienst AIVD en de CIE van de politie. Hieronder geven wij de kenmerken naast elkaar weer. Door tegelijkertijd bijvoorbeeld het eerste kenmerk van beide organisaties te behandelen, krijgt de lezer een duidelijk beeld van de belangrijkste verschillen tussen de veiligheidsdienst en de politie.

Het eerste kenmerk betreft de algemene taakstelling van de organisaties: een veiligheidsdienst richt zich op de bescherming van de nationale veiligheid en heeft een behoorlijke vrijheid bij het beoordelen van welke gevallen onder deze doelstelling vallen. De politie richt zich onder meer op het handhaven van de strafrechtrechtelijke rechtsorde, oftewel het opsporen van criminaliteit. De strafrechtelijke rechtsorde wordt gevormd door vooraf door de wetgever vastgestelde strafrechtelijke bepalingen. Daar waar de veiligheidsdienst veel ruimte heeft voor het invullen van diens taak, het enige criterium is namelijk de nationale veiligheid, wordt de politie aanzienlijk beperkt in haar mogelijkheden. Zij kan slechts optreden tegen de gedragingen die vallen onder de door de wetgever vooraf vastgestelde criteria die vervat zijn in delictsomschrijvingen.

Het tweede kenmerk betreft het middel waarmee de organisaties trachten het doel te bereiken. Omdat een aantasting van de nationale veiligheid desastreus kan zijn, zal een veiligheidsdienst zoveel mogelijk proberen dit te voorkomen. De meeste veiligheidsdiensten grijpen doorgaans niet zelf in om de bedreiging te voorkomen, maar waarschuwen (politieke) belangendragers en deze zullen daadwerkelijk (laten) ingrijpen. Veiligheidsdiensten handelen dus met name proactief en preventief door middel van het geven van voorwaarschuwingen (aan andere partijen) van mogelijk op handen zijnde bedreigingen van de nationale veiligheid. Voor het geven van voorwaarschuwingen is een goede informatiepositie noodzakelijk, en het opbouwen en in stand houden van een informatiepositie is dan ook een zelfstandig doel van de veiligheidsdiensten. Het geven van voorwaarschuwingen en de opbouw en het opbouwen en in stand houden van een goede (brede) informatiepositie zijn dan ook intrinsiek met elkaar verbonden. Aan de informatiepositie van de veiligheidsdiensten zitten nauwelijks grenzen, omdat de bedreiging van de nationale veiligheid niet vast omlijnd is. Zij richten zich dan ook op de ongekende dreiging, hetgeen betekent dat in theorie vrijwel alle informatie voor deze diensten relevant kan zijn. De traditionele politie doet echter niet aan het geven van voorwaarschuwingen, maar aan waarheidsvinding. Waarheidsvinding vereist een ander soort informatiepositie dan voorwaarschuwingen: het richt zich op wat er is gebeurd, en niet op wat er nog kan gaan gebeuren. Voor de politie is de opbouw en instandhouding van een informatiepositie dan ook niet zozeer een zelfstandig doel, maar is dit gericht op de waarheidsvinding. De informatiepositie van de traditionele politie kent wel duidelijke grenzen: het mag slechts gaan om informatie in relatie tot strafbare feiten in het licht van de materiële waarheidsvinding. Dit vloeit voort uit het verschil in taken tussen beide organisaties. De politie mag haar bevoegdheden namelijk slechts inzetten in het kader van het opsporen van strafbare feiten. Omdat de toepassing van de bevoegdheden leidt tot een inbreuk in de persoonlijke levenssfeer van de burger of anderszins tot een beperking van diens rechten, vindt de toepassing ervan slechts plaats indien hier een concrete aanleiding voor is: er moet sprake zijn van een verdenking. Deze aanleiding is traditioneel een concreet gepleegd strafbaar feit, hetgeen de politie een reactieve organisatie maakt. Indien de politie daadwerkelijk een inbreuk op de rechtsorde constateert, dan kan zij zelfstandig ingrijpen.

Het derde kenmerk ziet op het werkproces van de organisaties. Een veiligheidsdienst werkt over het algemeen volgens de fasen van de intelligence-

cyclus: (1) het opstellen van een intelligence-agenda (*requirements*), (2) planning en opdracht, (3) verzamelen van inlichtingen, (4) verwerken van inlichtingen, (5) analyseren en tot slot (6) verspreiden van analyseproducten. Dit leidt tot het bijstellen van de inlichtingenbehoeften van de klant en het opstellen van een nieuwe intelligence-agenda; daarmee is de cyclus rond. Deze traditionele intelligence-cyclus geeft echter te weinig inzicht in (1) de complexe realiteit van de veiligheidsdiensten en (2) de relatie tussen de veiligheidsdienst en de context. Vanwege deze tekortkomingen van de traditionele intelligence-cyclus vullen wij de cyclus aan door ook de context eraan toe te voegen en de fasen onderling met elkaar te verbinden, waardoor het model meer recht doet aan de realiteit van de veiligheidsdiensten.

Het werkproces van de politie in het kader van de opsporing van strafbare feiten wordt echter niet gekenmerkt door de intelligence-cyclus, maar door het proces van het opsporingsonderzoek. De politie verzamelt bewijs ten behoeve van verdenkingen en veronderstellingen omtrent gepleegde strafbare feiten, teneinde een verdachte aan te houden en deze te (laten) vervolgen. Het verzamelen van bewijs is dan ook iets heel anders dan het verzamelen van informatie ten behoeve van risico-inschattingen (intelligence). Het is in verregaande mate gereguleerd en de vaststelling van wat als (strafrechtelijk relevante) waarheid wordt gezien, geschiedt door de rechter en niet door de politie of het OM.

Het vierde kenmerk ziet op de relatie van de beide organisaties met externen, en daarmee ook op de onderlinge relatie tussen de veiligheidsdienst en de politie. Het is ook een essentieel kenmerk omdat het in belangrijke mate de betreffende organisatie typeert. Voor de veiligheidsdiensten is dit vierde kenmerk de geheimhouding. Deze heeft vaak operationele redenen, maar is daarnaast ook het gevolg van binnen bureaucratieën geldende concurrentieoverwegingen. Het vierde kenmerk van de politie is echter transparantie: er wordt een inbreuk gemaakt op de rechten van een individu, en alhoewel dit in eerste instantie vaak heimelijk plaatsvindt (bijvoorbeeld door middel van een telefoontap of infiltratie), uiteindelijk dient het politieoptreden transparant te zijn. De strafrechter dient te weten welke feiten de politie heeft verzameld en hoe zij dat heeft gedaan, en de verdachte moet zich kunnen verweren tegen hetgeen hem of haar ten laste wordt gelegd. Daarnaast is er ook dikwijls transparantie naar de buitenwereld toe. Dit zijn de zogenoemde principes van interne en externe openbaarheid, oftewel de eis tot transparantie van het opsporingsproces.

De mate waarin de vier kenmerken van de veiligheidsdienst een onderdeel vormen van IGP, bepaalt de mate waarin er sprake is van een vermenging van functie tussen veiligheidsdienst en de politie.

3| De Algemene Inlichtingen- en Veiligheidsdienst

In dit hoofdstuk beantwoorden wij evenals in hoofdstuk twee OV1: *Wat zijn de traditionele kenmerken van veiligheidsdiensten en de politie?* Wij doen dit door de HP-kenmerken uit hoofdstuk twee verder uit te werken aan de hand van onze bevindingen betreffende de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). De afgelopen jaren zijn er diverse publicaties verschenen over de geschiedenis en de dagelijkse werkzaamheden van de AIVD. Dit hoofdstuk combineert inzichten uit deze publicaties en beschrijft de organisatie van deze Nederlandse veiligheidsdienst tot en met de politiek-bestuurlijke context. We doen dit als volgt.

Wij behandelen ten eerste de organisatie van de AIVD (sectie 3.1). Daarna gaan wij in op de activiteiten van de AIVD (sectie 3.2). Vervolgens beschrijven wij de informatieverzameling door de AIVD (sectie 3.3). Na de informatieverzameling behandelen wij het verwerken van de verzamelde inlichtingen (sectie 3.4). Omdat dit onderzoek de verhouding tussen de Nederlandse veiligheidsdienst en een onderdeel van de Nederlandse opsporingsorganisatie behandelt, besteden wij kort aandacht aan de rol van AIVD-informatie in het Nederlandse strafproces (sectie 3.5). Het volgende onderwerp van het hoofdstuk gaat over de relatie met een organisatieonderdeel dat in een bijzondere verhouding tot de AIVD en de politie staat, te weten de Regionale Inlichtingendienst (RID, sectie 3.6). Daarna beschrijven wij de politiek-bestuurlijke context van de AIVD (sectie 3.7). Voor de beantwoording van OV1 combineren we tot slot de kenmerken uit het vorige hoofdstuk met de bevindingen van dit hoofdstuk (sectie 3.8).

3.1 Organisatie van de AIVD

In vergelijking met de politie is de AIVD een vrij kleine organisatie. Er werken op het moment van schrijven (augustus 2011) ongeveer 1100 mensen voor de dienst. In het kader van reorganisaties en ontwikkelingen die betrekking hebben op terrorismebestrijding is het de bedoeling om uiteindelijk over 1500 medewerkers te beschikken.

Tot 2010 bestond de AIVD uit zes directies. Deze directies waren verdeeld over de verschillende taken. Om de gedachte te bepalen geven we twee voorbeelden: een directie Democratische Rechtsorde en een directie Staatsveiligheid. Inmiddels spreekt de dienst niet meer van 'directies' maar van 'eenheden' en '*business units*'.[71] De directies zijn getransformeerd in negen eenheden en twee *business-units*.[72] De belangrijkste eenheid voor dit onderzoek is (1) de Eenheid Binnenlandse Veiligheid. Hierin zijn de oude directies Democratische Rechtsorde, Staatsveiligheid en Veiligheidsbevordering opgenomen. Deze eenheid is verantwoordelijk voor de bescherming van de democratische rechtsorde, de staatsveiligheid en de veiligheidsbevordering. Bij de taakuitvoering van de eenheid Binnenlandse Veiligheid komen de AIVD en de politie elkaar het meeste tegen en hier is de noodzaak tot afstemming van activiteiten dan ook het grootst. Op de website van de AIVD is te lezen waarop deze eenheid zich richt: "(…) *het waarborgen van een afdoende mate*

[71] www.aivd.nl, gezien op 26 november 2009.
[72] Informatie over de eenheden en business units zijn afkomstig van de website van de dienst: www.aivd.nl, gezien op 26 november 2009. Anders dan deze omschrijving is er van deze hele verandering ten opzichte van de directie-structuur geen informatie te vinden.

van risicobeheersing op de taakvelden Contra-terrorisme, Radicaliseringstendensen, Contra-inlichtingen, Rechts-extremisme, Links-extremisme, Dierenrechtenextremisme en Veiligheidsbevordering."[73] Deze taak van de eenheid Binnenlandse Veiligheid wordt ook wel de 'A-taak' genoemd. De naam verwijst naar de taakstelling van de dienst in de Wet op de Inlichtingen- en Veiligheidsdiensten van 2002 (verder: WIV 2002), te weten artikel 6 lid 2 sub a WIV 2002 (zie verder subsectie 3.2.1).

Voor de volledigheid noemen we de overige acht eenheden eveneens, alsmede de twee *business units.* De eenheid Binnenlandse Veiligheid (1) kennen we. Daarnaast gaat het om: (2) de eenheid Dienstencentrum, verantwoordelijk voor alle standaard dienstverlening binnen de AIVD, zoals de personele en financiële administratie; (3) de eenheid Informatiemanagement, belast met het leveren van duurzame ICT-voorzieningen conform de vraag van de AIVD; (4) de eenheid Inlichtingen Buitenland, de zogenoemde 'offensieve inlichtingeneenheid' die belast is met het verzamelen van inlichtingen omtrent het buitenland; (5) de eenheid Kenniscentrum Verbetermanagement en Innovatie, een managementafdeling onder meer belast met de ontwikkeling van verbeter- en veranderingsprocessen; (6) de eenheid Regie, belast met de interne samenhang en samenwerking; (7) de eenheid Strategie en Beleid, (8) een ondersteunende beleidsstaf die de leiding van de dienst ondersteunt; (9) de eenheid Trendanalyse en Fenomeenonderzoek die zich richt op het analyseren van fenomenen die een bepaalde eenheid overstijgen. De twee *business-units* hebben een taak op (1) het vlak van informatiebeveiliging en (2) het uitvoeren van veiligheidsonderzoeken.

3.2 De activiteiten van de AIVD

De Commissie Havermans (2004: 23) geeft kernachtig aan waarom een inlichtingen- en veiligheidsdienst nodig is: "*Een inlichtingen- en veiligheidsdienst is noodzakelijk om een democratische rechtsstaat te beschermen tegen bedreigingen van de nationale veiligheid."* Nu klinkt dit op zichzelf vrij logisch. In hoofdstuk twee stond ook al beschreven dat dit de taak is van elke (inlichtingen- en) veiligheidsdienst, dus ook van de AIVD. Maar toch geeft dit niet echt duidelijkheid omtrent de taak van de AIVD. Want wat verstaat men eigenlijk onder 'nationale veiligheid?' De invulling van dit begrip bepaalt in hoeverre iets een onderwerp is voor de AIVD. Inzicht in de reikwijdte van het begrip geeft ook inzicht in de taakscheiding tussen veiligheidsdiensten en opsporingsdiensten: de politie richt zich immers op criminaliteit, en niet op de bescherming van de nationale veiligheid. Dit lijkt voor de hand liggend, maar we constateren toch dat dit centrale begrip in de sporadische discussies over de scheiding tussen veiligheidsdiensten en opsporingsdiensten nauwelijks een rol speelt. Derhalve begint ons onderzoek over de genoemde scheiding helemaal aan het begin. Het eerste aanknopingspunt voor het bepalen van de reikwijdte van 'nationale veiligheid' is de wettelijke taakstelling voor de AIVD zoals bepaald in de WIV 2002.

In de volgende subsecties beschrijven wij allereerst de functie van de AIVD en de algemene juridische taakstelling zoals beschreven door de WIV 2002 (subsectie 3.2.1). We staan daarna kort stil bij wat er onder nationale veiligheid moet worden verstaan (subsectie 3.2.2). Vervolgens gaan wij dieper in op wat het 'nationale' van het beschermen van de nationale veiligheid inhoudt (subsectie 3.2.3). Daarna

[73] www.aivd.nl, gezien op 26 juli 2010. Zie ook de Commissie Havermans (2004: 128).

behandelen wij de zogenoemde 'A-taak' (subsectie 3.2.4). Wij werken deze A-taak vervolgens verder uit voor het onderwerp terrorisme (subsectie 3.2.5).

3.2.1 De functie en taak volgens de WIV 2002

De functie van de AIVD is tweeledig: aan de ene kant is het een functioneel directoraat-generaal dat ressorteert onder het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De AIVD is in dit opzicht dus een beleidsorganisatie: een ambtelijke bureaucratische organisatie belast met het vaststellen en uitvoeren van een publieke taak. Formeel is de hoogste leidinggevende van de dienst dan ook een directeur-generaal, maar zo wordt hij in de praktijk niet genoemd. De benaming van de hoogste leidinggevende van de dienst is 'hoofd AIVD'. Samen met het plaatsvervangend hoofd woont het hoofd AIVD de wekelijkse vergadering van de Bestuursraad bij (Commissie Havermans 2004: 28). Aan de andere kant is de AIVD een operationele dienst. Deze hoofdfunctie van de AIVD wordt door de Commissie Havermans (2004: 24-25) als volgt geformuleerd: "(*de hoofdfunctie van de AIVD is) door gegevensverstrekking andere overheidsorganen en/of particulieren in staat te stellen adequate maatregelen te treffen, hetzij met het oog op het wegnemen van een dreiging, hetzij met het oog op het verhogen van de eigen weerstand c.q. beveiliging*." De functie is belangrijker voor ons onderzoek dan het bovengenoemde functioneel directoraatgeneraalschap, omdat de activiteiten die in het kader van de operationele hoofdfunctie worden ontplooid direct in relatie staan tot de verhouding tussen de AIVD en de CIE. Bij deze operationele hoofdfunctie spelen met name de taakbepalingen van artikel 6 WIV 2002 een belangrijke rol.

Artikel 6 lid 2 WIV 2002 behelst de taakstelling van de dienst. Het artikellid maakt een onderscheid in vijf verschillende taken, elk aangegeven met een letter (A t/m E). Artikel 6 lid 2 luidt als volgt.

"De Algemene Inlichtingen- en Veiligheidsdienst heeft in het belang van de nationale veiligheid tot taak:
A: het verrichten van onderzoek met betrekking tot organisaties en personen die door de doelen die zij nastreven, dan wel door hun activiteiten aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat;
B: het verrichten van veiligheidsonderzoeken als bedoeld in de Wet veiligheidsonderzoeken;
C: het bevorderen van maatregelen ter bescherming van de onder a genoemde belangen, waaronder begrepen maatregelen ter beveiliging van gegevens waarvan de geheimhouding door de nationale veiligheid wordt geboden en van die onderdelen van de overheidsdienst en van het bedrijfsleven die naar het oordeel van Onze ter zake verantwoordelijke Ministers van vitaal belang zijn voor de instandhouding van het maatschappelijk leven;
D: het verrichten van onderzoek betreffende andere landen ten aanzien van onderwerpen die door Onze Minister-President, Minister van Algemene Zaken, in overeenstemming met Onze betrokken Ministers zijn aangewezen."
E: het opstellen van dreigings- en risicoanalyses op verzoek van Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties en Onze Minister van Justitie gezamenlijk ten behoeve van de beveiliging van de personen bedoeld in de artikelen 6, derde lid, onderdeel b, en 38, eerste lid, onderdeel c, van de Politiewet 1993 en de bewaking en

beveiliging van de objecten en de diensten die zijn aangewezen op grond van artikel 15a van die wet."

Als het gaat om het vaststellen van de reikwijdte van 'nationale veiligheid', valt op dat alle taken uit artikel 6 met elkaar gemeen hebben dat ze worden verricht in het belang van de nationale veiligheid. De reikwijdte van het begrip 'nationale veiligheid' wordt dan ook bepaald door de nadere uitwerking van de werkzaamheden van de dienst in de taakartikelen, met name daar waar het de A-taak of de C-taak betreft.[74] Dit maakt van 'nationale veiligheid' een overkoepelend begrip. Het gevolg hiervan is dat andere criteria genoemd in artikel 6 WIV 2002, zoals 'andere gewichtige belangen' en 'vitale belangen' eveneens onder het begrip 'nationale veiligheid' vallen. Derhalve is het nog steeds niet duidelijk wat precies onder 'nationale veiligheid' wordt verstaan.

3.2.2 Nationale veiligheid

Hieronder proberen we tot een verdere afbakening van het begrip 'nationale veiligheid' te komen. Uit de wetsgeschiedenis volgt geen vastomlijnde definitie van dit begrip. 'Nationale veiligheid' is een breed, veelomvattend begrip waar geen nadere definitie van wordt gegeven in wetgeving of jurisprudentie. Dit gebeurt zo om de dagelijkse werkzaamheden van de dienst niet teveel te belemmeren.[75] Daarnaast wijst de wetgever ook op de 'tand des tijds', die zich niet houdt aan een vast omlijnde en limitatieve opsomming van welke feiten wel en welke niet onder 'nationale veiligheid' vallen.[76] Toch zijn er wel enige aanknopingspunten om vast te stellen wanneer er sprake is van nationale veiligheid.

Zo wijst de minister van Binnenlandse Zaken en Koninkrijksrelaties met betrekking tot de achtergrond van de term 'nationale veiligheid' naar het EVRM, meer specifiek artikel 8. Artikel 8 ziet kort gezegd op de bescherming van de persoonlijke levenssfeer; de privacy dus. Het EVRM biedt staten de mogelijkheid om een inbreuk te maken op het mensenrecht privacy onder andere in gevallen van nationale veiligheid.[77] Het Europees Hof voor de Rechten van de Mens (EHRM) definieert het begrip echter niet in de jurisprudentie, maar uit de casus blijken wel dat veel verschillende fenomenen onder de noemer 'nationale veiligheid' kunnen worden geschaard, zoals het schenden van staatsgeheimen, het oproepen tot en het goedkeuren van het gebruik van geweld en het verrichten van terroristische activiteiten.[78] Het EHRM laat aan de lidstaten voorts een ruime '*margin of appreciation*' voor de beoordeling of iets tot de nationale veiligheid behoort. Met andere woorden, wat vandaag onder 'nationale veiligheid' wordt verstaan, kan morgen weer geheel veranderd zijn. In dit opzicht lijkt de houding van het EHRM op die van de Nederlandse wetgever, en de reden moet worden gezocht in de werkbaarheid voor de veiligheidsdiensten.

Veiligheidsdiensten hebben een brede discretionaire bevoegdheid die hen in staat stelt om in te schatten of bepaalde organisaties of individuen een bedreiging voor de nationale veiligheid vormen. Nu de wetgever ervoor heeft gekozen om geen nadere

[74] *Kamerstukken II*, 1999/2000, 25 877, nr. 14, p. 15.
[75] *Kamerstukken II*, 1999/2000, 25 877, nr. 59, p. 1-2.
[76] *Kamerstukken II*, 1999/2000, 25 877, nr. 14, p. 15.
[77] Het artikel geeft ook andere gronden voor het schenden van de privacy van burgers, zoals het onderzoeken van strafbare feiten (de opsporing).
[78] *Kamerstukken II*, 1999/2000, 25 877, nr. 59, p. 1-2.

definitie van 'nationale veiligheid' te geven, is het aan de AIVD zelf om per geval te bepalen of een persoon of organisatie een bedreiging voor de nationale veiligheid vormt. Aan een dergelijke brede definitie kleeft echter een bezwaar. Indien de AIVD zelf kan bepalen in welke gevallen er sprake is van een dreiging voor de nationale veiligheid, brengt dit het probleem met zich mee dat de dienst tot op zekere hoogte zelf zijn eigen mandaat kan vaststellen. De vraag die dan rijst is in hoeverre het stempel 'nationale veiligheid' consequent wordt toegepast bij (potentiële) bedreigingen van de nationale veiligheid. Het probleem is dat het voor de burger onduidelijk zal zijn in welke gevallen de veiligheidsdienst zal optreden.[79] Deze onzekerheid gecombineerd met een verregaande geheimhouding (en executieve bevoegdheden) maakte in het verleden veiligheidsdiensten, zoals de Stasi en de Gestapo, berucht en gevreesd.

Naast het doen van een beroep op de 'nationale veiligheid' kunnen staten (in het algemeen) ook in gevallen van (1) openbare veiligheid (*public safety*) en (2) bescherming van rechten en vrijheden van anderen (*the protection of rights and liberties of others*) inbreuken op de privacy van burgers maken. Volgens de Nederlandse overheid vallen deze twee gronden onder het begrip 'nationale veiligheid'. Drie voorbeelden van zaken van openbare veiligheid die vallen onder nationale veiligheid zijn terrorisme, gewelddadig activisme op openbare plaatsen en voetbalvandalisme met een maatschappelijk ontwrichtend karakter. Voor de beoordeling of het hier een AIVD-taak betreft, moet worden bezien of er een gewichtig belang van de staat in het geding is.[80] Het beschermen van de gemeenschapsveiligheid kan dus ook tot de taak van de AIVD behoren, mits er een belang van de staat in het geding is.[81] Dit zal bij massamoorden, grootschalige verstoringen van de openbare orde door bijvoorbeeld een extreem-rechtse (of extreem-linkse) demonstratie al snel het geval zijn. Een voorbeeld van het beschermen van rechten en vrijheden van anderen die vallen binnen nationale veiligheid is de schending van grondrechten en een onderwerp als mensensmokkel.[82] Andere schendingen van grondrechten kunnen hier ook onder vallen. Voor een verder inzicht in concrete zaken die door de AIVD tot de nationale veiligheid worden gerekend, verwijzen wij naar de jaarverslagen van de dienst.[83]

3.2.3 Het 'nationale' van nationale veiligheid

Een belangrijke consequentie (en beperking) van het verbinden van de taakstelling van de veiligheidsdiensten met het begrip 'nationale veiligheid' ligt in het nationale: een veiligheidsrisico op lokale of regionale schaal wordt alleen een zaak voor de AIVD indien er een nationaal element in de dreiging ligt verscholen. Een voorbeeld is het bedreigen van een burgemeester of een andere lokale politicus vanwege een lokaal

[79] De geheimhouding van de dienst betekent echter vaak dat de burger van het optreden weinig zal merken. Dit laat onverlet dat de AIVD met het inzetten van zijn bevoegdheden een inbreuk op de persoonlijke levenssfeer maakt, iets waar in een democratische rechtsstaat niet lichtzinnig mee moet worden omgegaan. Bovendien moet de inbreuk bij wet (*law*) zijn voorzien en die wet moet toegankelijk (*accessible*) en voorzienbaar (*foreseeable*) zijn (zie voor een uitgebreide behandeling van deze begrippen Loof 2005: 204 e.v.).

[80] *Kamerstukken II*, 1999/2000, 25 877, nr. 14, p. 14-15.

[81] Fouché en Brodeur bestempelden de bescherming van de openbare veiligheid echter als het kenmerk van *low policing*. Volgens de Nederlandse regering valt dit echter ook onder *high policing*. Zie hoofdstuk twee.

[82] *Kamerstukken II*, 25 877, nr. 14, p. 14-15,

[83] Deze zijn te downloaden van: www.aivd.nl.

dispuut. Dit zal in het algemeen buiten het taakgebied van de AIVD vallen, omdat het een lokale aangelegenheid betreft. Het bedreigen van een minister valt daarentegen wel binnen het taakgebied van de dienst, omdat een dergelijke bedreiging op nationaal niveau plaatsvindt. Maar ook het bedreigen van een burgemeester als protest tegen het instituut van de burgemeester, valt onder de taakstelling van de AIVD. Zo'n bedreiging raakt aan een vitaal belang voor de staat en vormt wellicht een bedreiging voor het voorbestaan van de democratische rechtsstaat (de A-taak). Gevallen van mogelijke corruptie of andere integriteitsgevallen met betrekking tot lokale of provinciale politici of ambtenaren zijn overigens ook een taak voor de AIVD: integriteitsproblemen met betrekking tot lokale of provinciale politici en ambtenaren worden in het jaarverslag van 1999 gezien als intrinsiek verbonden met de integriteit van de publieke sector in het algemeen en vallen daarmee onder de taakstelling van de dienst.[84] Met andere woorden, een bedreiging vormt een gevaar voor de democratische rechtsorde dan wel voor de veiligheid van de staat 'indien het om kwesties gaat die een uitstraling naar nationaal niveau kunnen hebben'.[85]

Zoals reeds eerder is opgemerkt vallen de taakbepalingen van artikel 6 WIV 2002 ook onder het begrip nationale veiligheid. Voor ons onderzoek is met name de A-taak van groot belang. Binnen de uitvoering van deze taak kunnen zich naast onderzoeken van de AIVD ook opsporingsonderzoeken van de politie bevinden (inclusief het CIE-werk in de voorfase). Deze onderzoeken kunnen elkaar raken, mogelijk overlappen en beïnvloeden. Als terrorisme en georganiseerde criminaliteit tot het taakgebied van de AIVD kunnen worden gerekend, dan is dat op basis van dit artikel. Daarom beperken we ons in ons onderzoek tot deze A-taak en laten we de andere taken buiten beschouwing.

3.2.4 De A-taak

Wij herhalen hier de A-taak van artikel 6 lid 2a WIV 2002: "*het verrichten van onderzoek met betrekking tot organisaties en personen die door de doelen die zij nastreven, dan wel door hun activiteiten aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat.*"

Net als bij de invulling van het begrip 'nationale veiligheid' is de A-taak van de dienst ruim geformuleerd zodat de interpretatie ervan in de loop van de tijd kan veranderen. De kern van de A-taak is het beschermen van gewichtige belangen van de staat. Het voortbestaan van de democratische rechtsorde en de veiligheid van de staat zijn hiervoor een belangrijk onderdeel (Commissie Havermans 2004: 121). Andere belangen van de staat zijn dan ook pas 'gewichtige belangen' als zij wat zwaarte betreft vergelijkbaar zijn met de criteria "democratische rechtsorde" en "de veiligheid van de staat". Drie voorbeelden hiervan zijn: (1) terrorisme, (2) grootschalige verstoring van de openbare orde (indien ze heimelijk zijn voorbereid met als doel het veroorzaken van politieke instabiliteit) en (3) activiteiten ontplooid op Nederlands grondgebied die zijn gericht op een gewelddadige omverwerping van een buitenlands regime.[86] Deze voorbeelden geven duidelijk de link aan met de term 'nationale veiligheid': het betreft gevallen van openbare veiligheid en het heeft (inter)nationale strekking.

[84] Zie: jaarverslag BVD 1999, *Kamerstukken II*, 1999/2000, 25 877, nr. 14, p. 8.
[85] *Kamerstukken II*, 1999/2000, 25877, nr. 14, p. 8.
[86] *Kamerstukken II,* 2000/01, 25 877, nr. 59, p. 2.

Uit het bovenstaande volgt dat de AIVD als taak heeft het beschermen van de nationale veiligheid door middel van verrichten van onderzoek. De vraag rijst wat onder 'het verrichten van onderzoek' moet worden verstaan. In een oude bepaling met betrekking tot de A-taak werd gesproken van 'het verzamelen van gegevens' in plaats van 'het verrichten van onderzoek'. Het verzamelen van gegevens is een onderdeel van het verrichten van onderzoek en valt meer specifiek onder de definitie van 'gegevensverwerking' uit artikel 1 WIV 2002. De wetgever is van mening dat 'het doen van onderzoek' meer recht doet aan het centrale karakter van de taak van de AIVD dan de oude omschrijving van 'verzamelen van gegevens', hetgeen overigens niet betekent dat er feitelijk veel is veranderd.[87] Het verzamelen van informatie is nog steeds de kernactiviteit van de AIVD: in tegenstelling tot bijvoorbeeld de opsporingsdiensten kan de dienst weinig anders doen. Hij kan bijvoorbeeld geen aanhoudingen verrichten. Dit heeft met name te maken met de specifieke functie van de dienst in het kader van de taakstelling: de dienst heeft een waarschuwingsfunctie. Veiligheidsdiensten dienen in de eerste plaats andere partijen in een tijdig stadium te waarschuwen voor dreigingen zodat deze kunnen voorkomen dat een aantasting van de nationale veiligheid ook daadwerkelijk plaatsvindt.[88] Het is dus niet de dienst die ingrijpt en daadwerkelijk een aantasting van de nationale veiligheid voorkomt, maar een derde, zoals de politie of de IND, die op basis van adviezen van de dienst in actie komt. De AIVD zal dus doorgaans niet zelf personen aanhouden of op een andere manier direct ingrijpen.

3.2.5 Terrorisme

Na 11 september 2001 is de bestrijding van terrorisme de belangrijkste taak van de dienst geworden. Dit is ten koste gegaan van andere aandachtsgebieden zoals aandacht voor gewelddadig politiek activisme (Commissie Havermans 2004: 140). Het behoeft geen uitgebreid betoog dat terroristische aanslagen een gevaar vormen voor de democratische rechtsorde of andere gewichtige belangen van de staat. In dit kader is het derhalve zinvol om stil te staan bij wat de AIVD precies onder het begrip 'terrorisme' verstaat. Het is immers denkbaar dat de AIVD en de politie andere definities van terrorisme hanteren. We behandelen achtereenvolgens (A) de definitie van terrorisme volgens de AIVD, (B) de verdere invulling van dat begrip, (C) het radicaal-islamitisch terrorisme en (D) andere vormen van terrorisme en gerelateerde onderwerpen. Tot slot gaan wij kort in op (E) georganiseerde criminaliteit en de AIVD.

A: Definitie van terrorisme volgens de AIVD

Terrorisme is volgens de dienst: "*het plegen van of dreigen met op mensenlevens gericht geweld of het aanrichten van ernstige maatschappijontwrichtende zaakschade, met als doel maatschappelijke veranderingen te bewerkstelligen en politieke besluitvorming te beïnvloeden.*" Deze definitie wijkt af van de strafrechtelijke definitie van terrorisme, waarbij het *terroristisch oogmerk* centraal

[87] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 9. In de praktijk bestaat er overigens een vorm van onderzoek die niet in de wet terug te vinden is: naslag. Naslag is niet hetzelfde als 'het doen van onderzoek'. Bij naslag gaat de AIVD de eigen systemen na om te bezien of een persoon in daarin voorkomt (Commissie Havermans 2004: 122-123). Naslag is echter voor dit onderzoek niet relevant en zal verder buiten beschouwing worden gelaten.
[88] *Kamerstukken I,* 2001/02, 25 877, nr. 58a, p. 14.

staat bij de beoordeling of bepaalde misdrijven als terroristische misdrijven kunnen worden aangemerkt.[89] De AIVD kijkt echter niet door deze strafrechtelijke bril naar terrorisme. Het doel van de definitie van de AIVD is veel meer om duidelijkheid te scheppen in de gehanteerde terminologie: wanneer spreken we van terrorisme en wanneer niet. De dienst zal proberen terrorisme als fenomeen te begrijpen, alleen dan is het immers mogelijk om de dreiging die ervan uitgaat in te schatten. Op het eerste gezicht lijkt de definitie die de politie hanteert eenzelfde doel te hebben. Ook daar zal men aan de hand van een bepaalde toetssteen (de daar gehanteerde definitie) moeten beoordelen in welke gevallen er sprake is van terrorisme en in welke gevallen niet. Juridische definities hebben echter niet zozeer een verklarende functie, maar hebben als doel het omvormen (en herdefiniëren van) tamelijk complexe sociale fenomenen tot juridisch relevante zaken die vatbaar zijn voor een rechterlijke toetsing. Een strafrechtelijke definitie heeft evenwel veel meer een poortwachterfunctie: pas als er sprake is van een terroristisch oogmerk mogen de ruime bevoegdheden die aan de politie zijn toegekend in het kader van terrorismebestrijding worden ingezet. Dit verschil in definities kan in de praktijk belangrijke gevolgen hebben voor de verhouding tussen politie en veiligheidsdiensten. Immers, iets kan terrorisme zijn onder de definitie van de één en dat niet zijn onder de definitie van de ander. Zulk een verschil kan de onderlinge communicatie behoorlijk bemoeilijken. Zo behoeft de AIVD niet aan te tonen dat iets terrorisme is voordat hij bevoegdheden kan toepassen: het vaststellen of er sprake is van een bedreiging van de nationale veiligheid is immers voldoende. In de empirische hoofdstukken komen wij uitvoerig terug op de verschillen tussen de AIVD en de politie met betrekking tot de gehanteerde terminologie en de gevolgen daarvan voor de praktijk van de bestrijding van terrorisme en georganiseerde criminaliteit. Wij zullen nu de invulling van de definitie van terrorisme door de AIVD behandelen.

B: Invulling definitie door AIVD

De AIVD vult de definitie van 'terrorisme' in door een opsomming van de volgende onderwerpen: (1) radicaal-islamitisch terrorisme, (2) 'klassiek' terrorisme, (3) Nucleair, Chemische, Biologische en Radioactieve terrorisme, oftewel NCBR-terrorisme, (4) migratie gerelateerd aan terrorisme en (5) financiering van terrorisme. Hieruit kan worden geconcludeerd dat dierenrecht-activisme en andere vormen van radicaal activisme volgens de AIVD geen terrorisme zijn. Groeperingen die betrokken zijn bij deze vormen van activisme maken zich volgens de AIVD dus niet schuldig aan terrorisme zolang ze hun geweld niet richten op mensenlevens of het aanrichten van maatschappijontwrichtende zaakschade.[90] Van dit laatste is geen sprake volgens de AIVD indien bijvoorbeeld hokken van nertsen worden opengezet of kleine vernielingen en brandstichting plaatsvinden. Hiermee is overigens niet gezegd dat

[89] Artikel 83a WvSr: "*Onder terroristisch oogmerk wordt verstaan het oogmerk om de bevolking of een deel der bevolking van een land ernstige vrees aan te jagen, dan wel een overheid of internationale organisatie wederrechtelijk te dwingen iets te doen, niet te doen of te dulden, dan wel de fundamentele politieke, constitutionele, economische of sociale structuren van een land of een internationale organisatie ernstig te ontwrichten of te vernietigen."* Een duidelijk verschil met de AIVD definitie is het ontbreken van het criterium 'op mensenlevens gericht geweld'. De juridische definitie spreekt echter over het oogmerk 'vrees aan te jagen', een bestanddeel dat in de AIVD definitie weer ontbreekt.

[90] Deze 'zaaksschade' is door de dienst toegevoegd in navolging van het Europees kaderbesluit terrorisme. Oorspronkelijk zag de dienst dus enkel het plegen van of dreigen met op mensenlevens gericht geweld met als doel politieke of maatschappelijke veranderingen te bewerkstellingen als terrorisme. Hij hanteerde met andere woorden een smalle definitie. Zie Abels (2007: 126).

dierenrecht-activisme per definitie niet tot het taakgebied van de AIVD behoort. Dergelijke acties kunnen namelijk omvangrijke schade aanrichten aan bepaalde sectoren van het bedrijfsleven en als dit zo is raken ze gewichtige belangen van de staat. Ook dan is het volgens de AIVD echter geen terrorisme (het valt overigens wel onder de algemene taak van artikel 6 lid 2a WIV 2002).[91]

Terrorisme omvat overigens voor de AIVD meer dan radicaal-islamitische terroristische groeperingen en individuen zoals de Hofstadgroep en Mohammed B. Ook groeperingen zoals de Colombiaanse FARC, Turks-Koerdische PKK, Noord-Ierse IRA vallen onder de noemer 'terrorisme'. Het is echter het radicaal-islamitisch terrorisme dat volgens de Commissie Havermans (2004) de meeste aandacht krijgt van de dienst. Een relevante vraag is hier derhalve: wanneer is er volgens de AIVD sprake van radicaal-islamitisch terrorisme?

C: Radicaal-islamitisch terrorisme

De dienst spreekt zelf niet van 'radicaal-islamitisch terrorisme', maar van jihadistisch terrorisme. De definitie die de dienst hanteert luidt: "*Het plegen van of dreigen met op mensenlevens gericht geweld of het aanrichten van ernstige maatschappijontwrichtende zaakschade, met als doel om in het kader van de gewelddadige jihad maatschappelijke veranderingen te bewerkstelligen en politieke besluitvorming te beïnvloeden.*"[92] De dienst heeft dus aan de algemene definitie van terrorisme het element 'jihad' toegevoegd. Zaken als de aanslagen op de *Twin Towers* van 11 september 2001 vallen daarmee onder deze categorie. Een kernelement van de bovenstaande definitie is dan ook jihad: de gewapende strijd tegen vermeende vijanden van de islam, waarbij ter legitimering een beroep wordt gedaan op de islamitische rechtsleer.[93] De AIVD richt zich echter niet enkel op de harde-kern leden van een jihadistische groepering.

Omdat de AIVD (samen met andere partijen die bij terrorismebestrijding zijn betrokken) heeft gekozen voor een zogenoemde 'brede benadering' van terrorisme, richt hij zich zowel op het fenomeen terrorisme als op de elementen die er in bredere zin onderdeel van uitmaken (zie Commissie Havermans 2004: 129). Ook radicalisering wordt door de AIVD onderzocht. Hiervoor kent de AIVD een 'pijler radicaliseringstendensen' (RT-pijler, zie Commissie Havermans 2004: 139).[94] Voor de volledigheid geven wij nog een definitie die de AIVD hanteert, dit keer van radicalisering: "*(radicalisering is) de groeiende bereidheid om diepingrijpende veranderingen in de samenleving (eventueel op ondemocratische wijze) na te streven en/of te ondersteunen die op gespannen voet staan met of een bedreiging kunnen*

[91] Met betrekking tot radicaal dierenrechtactivisme hanteert de AIVD derhalve een andere definitie dan de politie. Bij de politie bestaat een neiging om ook radicaal dierenrechtactivisme onder de noemer van terrorisme te scharen. Dit heeft zoals gezegd er wellicht mee te maken dat de politie over meer bevoegdheden beschikt indien iets als terrorisme wordt aangeduid. De AIVD beschikt over dezelfde bevoegdheden, ongeacht of zij iets aanduidt als terrorisme of niet. Het maakt de operationele noodzaak om iets als 'terrorisme' te bestempelen bij de AIVD minder groot en verklaart wellicht een deel van het verschil tussen de AIVD en de politie daar waar het de definitie van terrorisme betreft.

[92] Zie voor een lijst van begrippen die de AIVD hanteert; https://www.aivd.nl/onderwerpen/taken-en/begrippenlijst, gezien op 4 november 2009.

[93] *Ibid.*

[94] Voorheen was dit de zogenoemde 'pijler Anti Integratieve krachten', oftewel de AI-pijler. Na de aanslagen van 11 september 2001 is deze pijler zich steeds meer gaan richten op radicaliseringsontwikkelingen gerelateerd aan contra-terrorisme. Zie Commissie Havermans (2004: 139).

vormen voor de democratische rechtsorde."[95] Bij radicalisering is weliswaar niet direct sprake van terrorisme, maar het is wel een aan terrorisme gerelateerd fenomeen en daarom valt het binnen de scope van de dienst. In een nota getiteld "*Van dawa tot jihad*" presenteerde de AIVD een theoretisch concept dat het mogelijk maakte om beleid te ontwikkelen dat was toegesneden op de aard en ernst van de dreiging (Abels 2007: 127). De AIVD deed in het document overigens voor het eerst zelf ook een aantal beleidsaanbevelingen, iets waarmee hij de grenzen van de taak van een veiligheidsdienst enigszins lijkt op te rekken.[96] In het kader van dit onderzoek brengen wij de activiteiten van de AIVD die zijn gericht op radicaliseringtendensen onder de noemer 'bestrijding van terrorisme'.

D: Andere vormen van terrorisme en gerelateerde onderwerpen

Naast het islamitisch terrorisme richt de AIVD zich ook op het 'klassieke' of 'oude' terrorisme. Dit zijn groeperingen zoals de Turks-Koerdische PKK, de Baskische ETA, en de Noord-Ierse IRA. Omdat de focus van de AIVD zich met name op de jihadistische netwerken richt, is er echter nog maar een beperkte capaciteit voor dit klassieke terrorisme (Commissie Havermans 2004: 134-135). De AIVD richt zich daarnaast ook op het NCBR-terrorisme. Vaak vallen organisaties die hiermee dreigen in de categorie van het jihadistisch terrorisme, maar dit hoeft niet het geval te zijn.

Verdere onderwerpen die aan terrorisme worden gekoppeld, zijn migratie en financiering. Terroristische netwerken maken niet zelden gebruik van dezelfde migratienetwerken als legitieme migranten. De AIVD houdt dit dan ook nauwlettend in de gaten. Vreemdelingen die aan terrorisme zijn gelieerd en die geen verblijfsstatus hebben, kunnen tot ongewenste vreemdelingen worden verklaard en worden uitgezet. Dit is dan ook een veelgebruikt middel in de bestrijding van terrorisme. Terroristische netwerken hebben voorts geld nodig. Daarom wordt het geldverkeer dat mogelijk door terroristen en terroristische organisaties wordt gebruikt door de AIVD in de gaten gehouden.

Uit het bovenstaande volgt dat de AIVD zich in belangrijke mate richt op het bestrijden van terrorisme, meer specifiek islamitisch terrorisme en de daaraan gerelateerde fenomenen zoals radicalisering, migratie en financiering. Het is niet overdreven om te stellen dat terrorismebestrijding vandaag de dag de belangrijkste taak is van de dienst, en dat terrorisme een waardige opvolger is van de oude vijand, het communisme.

E: Georganiseerde criminaliteit en de AIVD

Terrorisme mag dan wel een waardige opvolger zijn van het communisme als primair taakaccent van de AIVD, tussen de val van de Berlijnse muur en het daarmee wegvallen van de oude vijand en de aanslagen van 11 september 2001 die een nieuwe vijand opleverden zit echter ongeveer tien jaar. En het leek er in die tien jaar op dat

[95] Zie: https://www.aivd.nl/algemene-onderdelen/serviceblok/begrippenlijst/, gezien op 11 maart 2012. Wij merken op dat deze definitie ook van toepassing kan zijn op fenomenen die niet aan islamitisch-terrorisme zijn gerelateerd.

[96] Beleidsmakers dienen zich niet teveel te bemoeien met de inhoud van het werk van de veiligheidsdiensten, en de medewerkers van deze diensten dienen zich onzes inziens te onthouden van beïnvloeding van het beleid anders dan advisering. Zie ook hoofdstuk twee van dit boek voor een analyse van de taak van de veiligheidsdiensten. Zie ook Wirtz (2007). Over in hoeverre beleidsmakers en veiligheidsdiensten strikt gescheiden dienen te zijn lopen de meningen echter uiteen: zie sectie 2.1.

een heel andere vijand de plaats van het communisme zou overnemen: de georganiseerde criminaliteit. Zoals we in hoofdstuk één hebben aangegeven, richten wij ons op de verhouding tussen de AIVD en de CIE, waarbij de focus met name ligt bij de terrorismebestrijding. Omdat de CIE primair informatie verzamelt overde zware en georganiseerde criminaliteit, zullen wij ook kort stil staan bij de wijze waarop de AIVD met georganiseerde criminaliteit in aanraking komt.

Artikel 9 WIV 2002 laat er geen misverstand over bestaan: de ambtenaren van de AIVD hebben geen bevoegdheid tot opsporen, dit om een "*ongewenste vermenging van functies en daarbij behorende bevoegdheden*" te voorkomen.[97] Het kan daarom vreemd overkomen dat iets wat in de kern draait om strafbare feiten, zoals georganiseerde criminaliteit, toch tot het taakgebied van de AIVD kan behoren. Maar net als bij terrorisme (dat ook in de kern strafbare feiten betreft), gaat het de AIVD niet om de strafbare feiten *an sich*, maar met name om de vraag of de criminele organisaties een bedreiging voor het voortbestaan van de democratische rechtsorde vormen, of dat zij de veiligheid of andere gewichtige belangen van de staat in gevaar brengen. De AIVD onderzoekt in dit kader in hoeverre activiteiten van criminele organisaties afbreuk doen aan de integriteit van de staat en de samenleving.[98] Maar wat verstaat de AIVD eigenlijk onder georganiseerde criminaliteit? In tegenstelling tot bij terrorisme gebruikt de AIVD voor georganiseerde criminaliteit geen duidelijke definitie. Wij zullen deze vraag dan ook moeten beantwoorden aan de hand van de voorbeelden die we in de jaarverslagen en andere bronnen aantreffen.

In 1995 stelde de commissie Van Traa in haar eindrapportage vast dat, in tegenstelling tot wat destijds weleens in de media werd gesuggereerd, de BVD geen zelfstandig onderzoek verrichtte naar de zware en georganiseerde criminaliteit (Van Traa 1996, par. 8.8.5). Georganiseerde criminaliteit was volgens de door de commissie verhoorde medewerkers van de dienst geen zelfstandig aandachtsgebied van de BVD. Volgens de Commissie van Traa leek het er halverwege de jaren '90 op dat de dienst zich niet specifiek op het fenomeen van de georganiseerde criminaliteit richtte.

Uit de jaarverslagen van de BVD blijkt echter dat de dienst vanaf 1996 in toenemende mate aandacht kreeg voor georganiseerde criminaliteit. Verschillende criminaliteitsgerelateerde fenomenen werden door de BVD onderzocht. Het gaat om de volgende acht fenomenen: (1) de aantasting van de integriteit van de samenleving door middel van corruptie, investeren van met misdaad verkregen winsten, witwaspraktijken 'en dergelijke' (BVD 1996: 15); (2) de betrokkenheid van etnische minderheden bij de georganiseerde criminaliteit, waarbij de dienst zich met name richtte op de link tussen georganiseerde criminaliteit en 'etnopolitieke organisaties' en de eventuele betrokkenheid van vreemde mogendheden bij de georganiseerde criminaliteit (BVD 1997: 21; 1998: 32)[99]; (3) de handel in synthetische drugs; (4) de wapenhandel[100]; (5) het gebruik van contra-strategieën door criminele organisaties

[97] *Kamerstukken II*, 1997/98, 25 877, nr. 3, p. 15-16.
[98] *Kamerstukken II*, 1997/98, 25 877, nr. 8, p. 55-56.
[99] Specifiek onderzocht de BVD destijds de kwetsbaarheid van islamitische organisaties voor infiltratie vanuit 'de onderwereld'.
[100] Het zogenaamde Mikado-onderzoek van de BVD richtte zich ook op de wapenhandel. Een medewerker van de dienst infiltreerde in criminele netwerken en probeerde op die manier zicht te krijgen op onder andere de internationale handel in conventionele wapens. Met name de levering van dergelijke wapens aan gewelddadige politieke groeperingen zoals de IRA en de RaRa hadden de aandacht van de dienst. In het kader van dit onderzoek stuitte de dienst op informatie omtrent 'topcrimineel' Mink K. en vermeende contra-strategieën vanuit het criminele circuit. Het Mikado-onderzoek richtte zich dan ook op zowel de contra-strategieën van K. als de wapenhandel van die

(BVD 1996: 17); (6) mensenhandel, waarbij de BVD zich focuste op onder meer de betrokkenheid van buitenlandse inlichtingendiensten en politiek of religieus extreme organisaties; (7) de Russische georganiseerde criminaliteit vanwege de connectie tussen de politiek, het zakenleven (met name de financiële sector) en de georganiseerde criminaliteit (BVD 1997: 23); en tot slot (8) de strafzaak tegen de Surinaamse politicus Desi Bouterse, die ervan werd beschuldigd in cocaïne te hebben gehandeld en de invloed van het proces op de verhouding tussen Nederland en Suriname (dit kan tot de gewichtige belangen van de Nederlandse staat worden gerekend. Zie BVD 1999: 42).

In 2000 concludeerde de AIVD (destijds nog BVD geheten) kort maar krachtig dat uit de evaluatie van diverse onderzoeken naar georganiseerde criminaliteit volgde dat het fenomeen op zich geen aandachtsgebied voor de dienst behoort te zijn (BVD 2000: 37-38). De dienst hield de deur echter nog op een kier: in die gevallen waarin sprake is van een mogelijke bedreiging voor de integriteit van de openbare sector, zag de dienst nog wel een eigen toegevoegde waarde. Het jaarverslag uit 2000, dat in mei 2001 werd gepubliceerd, was een belangrijk breekpunt voor de dienst. Nog voor de aanslagen van 11 september 2001 concludeerde de dienst namelijk dat georganiseerde criminaliteit op zichzelf voor hem geen aandachtsgebied dient te zijn en dat de bestrijding daarvan zou worden overgelaten aan politie en justitie. De dreiging voor de nationale veiligheid die van de georganiseerde criminaliteit uitgaat, zou wel meevallen. Het is van belang dat de dienst dit voor de aanslagen van 11 september 2001 constateerde: er bestaat geen causaal verband tussen de opkomst van de nieuwe bedreiging van de nationale veiligheid (terrorisme) en het loslaten van de oude (georganiseerde criminaliteit).

Betekent dit nu dat de AIVD vandaag de dag geen rol speelt bij de bestrijding van zware en georganiseerde criminaliteit? Nee. Ook na 2000 blijft de dienst hier een rol spelen, al valt deze rol in vergelijking tot terrorismebestrijding vrijwel in het niet. Onderwerpen als wapenhandel en mensenhandel mogen anno 2012 nog steeds op de aandacht van de dienst rekenen, alhoewel het duidelijk is dat het fenomeen georganiseerde criminaliteit voor de dienst geen zelfstandig aandachtsgebied is. Voorts is terrorismebestrijding diffuus: het is namelijk niet altijd even duidelijk of een groepering het predicaat ‘terroristisch’ of ‘crimineel’ verdient. In de praktijk lijken groeperingen die officieel op de lijst van verboden terroristische organisaties staan zich ook bezig te houden met een breed scala van strafbare feiten waarmee zij wellicht ook tot de georganiseerde criminaliteit kunnen worden gerekend (zie Findlay 2008: 67-74; zie ook Dobbelaar en Koemans 2008). Er zijn veel voorbeelden van bijvoorbeeld Turks-Koerdische netwerken die grootschalig in heroïne handelen, geld witwassen, liquidaties plegen en zelfs afpersen. Hetzelfde geldt voor de Noord-Ierse IRA, die vandaag de dag meer wordt gezien als een vorm van georganiseerde criminaliteit dan als een terroristische organisatie (zie Curtis en Karazan 2002: 6-7). Er is ook sprake van een continuüm tussen de Amerikaanse *war on drugs* en de *war on terrorism*, waarbij inzichten die zijn opgedaan in de eerste ‘oorlog’ worden toegepast in de tweede. Kwalificaties als ‘narco-terrorisme’ zijn het gevolg van deze

---

groep. Later is de betrokken BVD-er overigens aangeklaagd voor het ‘lekken’ van staatsgeheime informatie naar bepaalde criminelen. Zie: Brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties van 24 januari 2006, 29876, nr. 11. Zie voor de zaak van de BVD-er: http://www.vn.nl/Archief/Justitie/Artikel-Justitie/OudAIVDer-Paul-Herrie-De-geheime-dienst-zwijgt-over-corruptie.htm, gezien op 20 december 2009.

ontwikkelingen (zie Andreas en Nadelmann 2006: 194-199). Georganiseerde criminaliteit en terrorisme lopen derhalve vaak door elkaar heen en een onderscheid tussen georganiseerde criminaliteit en terrorisme is in die gevallen niet goed meer te maken (zie ook: Dobbelaar en Koemans 2008).

3.3 Informatieverzameling

Daar waar buitenlandse 'geheime (inlichtingen)diensten', zoals de Mossad en de CIA, dikwijls de media halen vanwege betrokkenheid bij gewelddadige acties of andere 'interventies', haalt de Nederlandse AIVD de pers over het algemeen met een publicatie of een persbericht.[101] De reden hiervoor is met name dat de AIVD geen executieve bevoegdheden heeft; de dienst mag geen mensen aanhouden of handelingen verrichten die op één of andere manier bepaalde rechtsgevolgen voor individuen of organisaties teweeg brengen.[102] De dienst dient de 'belangendragers' (de officiële term voor de organisaties waaraan de dienst adviseert) zo snel mogelijk te informeren over bepaalde dreigingen, en heeft dus tot op zekere hoogte veel meer de rol van een informatiemakelaar. Het beschermen van de nationale veiligheid en de daarmee gepaard gaande noodzaak voor tijdige waarschuwingen van de AIVD aan anderen zijn volgens de wetgever van zo'n groot belang dat de dienst verregaande mogelijkheden heeft om informatie omtrent bedreigingen van de nationale veiligheid te verzamelen en de dreigingen in kaart te brengen. De bevoegdheden voor informatieverzameling van de dienst grijpen niet alleen diep in de persoonlijke levenssfeer van individuen in, ze kunnen ook betrekkelijk snel worden toegepast, sneller dan bijvoorbeeld de politie dat kan. Dit betekent echter niet dat de dienst bijvoorbeeld zomaar een ieder kan afluisteren. Voordat de AIVD een bevoegdheid kan toepassen is er een 'ernstig vermoeden' vereist van, kortgezegd, een gevaar voor gewichtige belangen van de staat.[103] Een vraag die nu rijst is wanneer de dienst een onderzoek start. Doet de AIVD dit op eigen initiatief of is hij afhankelijk van belangendragers die middels een melding aanleiding geven tot een ernstig vermoeden?

Als antwoord op een motie van de LPF en Groen Links om een lijst samen te stellen van welke instanties en personen gemachtigd zijn om de AIVD een verzoek danwel een opdracht tot onderzoek te verstrekken, zei de regering hierover het volgende: "*Een ieder kan bij de AIVD melding maken van feiten en omstandigheden die mogelijk aanleiding zijn voor een onderzoek in het kader van de A-taak. De AIVD bepaalt vervolgens zelf, in hoeverre het onderzoek past in zijn wettelijke taakomschrijving*".[104] Het publiceren van een limitatieve opsomming is ondoenlijk en

[101] Zie voor een overzicht van interventies in buitenlandse aangelegenheden door de CIA Weiner (2007).

[102] Overigens moet hierbij een onderscheid worden gemaakt tussen een buitenlandtaak en de binnenlandse taken van een dienst. Politieke inlichtingendiensten die in het buitenland actief zijn, zoals een CIA, houden zich niet aan de wetten die in het buitenland gelden. Spionage *an sich* is in vrijwel alle landen immers een strafbaar feit. Zij kunnen en mogen van de eigen wetgeving meer dan op het eigen grondgebied. Dit geldt ook voor de AIVD.

[103] Het strafrecht vereist een redelijk vermoeden van schuld aan een strafbaar feit. Zie hiervoor ook hoofdstuk vier. Het grote verschil tussen beiden is dat er bij een strafvorderlijke verdenking sprake moet zijn van strafbare feiten, hetgeen niet is vereist voor het ernstige vermoeden uit de WIV 2002. Zie MvA, *Kamerstukken I*, 2001/02, 25 877, nr. 58a, p. 14.

[104] *Kamerstukken II,* 2002/03 28811, nr. 10, p. 2. De motie van Groen Links en de LPF was ingediend naar aanleiding van het debat over de zaak De Roy van Zuydewijn op 12 maart 2003. Zie ook Commissie Havermans (2004: 123).

onwenselijk, nu het nooit op voorhand duidelijk zal zijn welke partij mogelijk voor de dienst interessante informatie bezit. Als het gaat om bedreigingen van de nationale veiligheid is een ieder dus gerechtigd om een melding bij de dienst te doen. Het is altijd de dienst zelf die bepaalt of iets valt onder de A-taak en dus een onderzoek verdient. Als de AIVD vervolgens besluit dat het een onderzoek waardig is, staan hem verschillende bevoegdheden ter beschikking. Deze bevoegdheden zijn vrij ruim, maar voor de toepassing ervan gelden verschillende regels. In de volgende subsecties komen deze bevoegdheden uitgebreid aan bod, beginnende bij de algemene bevoegdheid van artikel 17 WIV 2002: kort gezegd de bevoegdheid om vragen te stellen (3.3.1). Daarna behandelen wij de bijzondere bevoegdheden om heimelijk informatie te verzamelen (3.3.2). De inzet van de bijzondere bevoegdheden dient te voldoen aan de eisen van subsidiariteit (3.3.3) en proportionaliteit (3.3.4). Daarna gaan wij kort in op de praktijk van de toepassing van de bijzondere bevoegdheden en de procedures die door de dienst doorlopen dienen te worden (3.3.5). Eén van de belangrijkste bijzondere bevoegdheden die wij gedetailleerd beschouwen is het runnen van agenten, oftewel de *Human Intelligence* (HUMINT, subsecties 3.3.6 tot en met 3.3.8).

3.3.1 De algemene bevoegdheid van art. 17 WIV 2002

De AIVD heeft een algemene bevoegdheid om zich voor het verzamelen van gegevens te wenden tot een ieder die daarvoor volgens de dienst in aanmerking komt. Deze bevoegdheid is omschreven in artikel 17 lid 1 WIV 2002:

"*De diensten zijn bevoegd zich bij de uitvoering van hun taak, dan wel ter ondersteuning van een goede taakuitvoering, voor het verzamelen van gegevens zich te wenden tot:*
A: bestuursorganen, ambtenaren en voorts een ieder die geacht wordt de benodigde gegevens te kunnen verstrekken;
B: de verantwoordelijke voor een gegevensverwerking."

Het inwilligen van dit verzoek gebeurt op vrijwillige basis: men is dus niet verplicht om aan een dergelijk verzoek tegemoet te komen.[105] De dienst heeft overigens ook een algemene bevoegdheid om gegevens te verzamelen uit zogenoemde 'open bronnen' die voor iedereen toegankelijk zijn, alsmede niet-openbare gegevensverzamelingen, zoals gegevens uit de Gemeentelijke Basisadministratie en de politiedatabanken (Van der Bel et al. 2007: 266).

Diverse organisaties en individuen beschikken over informatie die voor de AIVD belangrijk kan zijn. Bestuursorganen en particulieren verzamelen informatie met specifieke doelen. Zo zal een bedrijf een klantenbestand bijhouden voor de interne bedrijfsvoering of voor bijvoorbeeld reclamedoeleinden. Luchtvaartmaatschappijen registreren diverse soorten gegevens onder het reserveringsnummer van hun klanten, met als doel het zo goed mogelijk afstemmen van te verlenen goederen en diensten op de wensen en voorkeuren van de passagier. De Kamer van Koophandel houdt een handelsregister bij onder meer ter bevordering van de rechtszekerheid: ondernemers kunnen nagaan of iemand wel bevoegd is om

[105] Voor dienstverleners op het gebied van telecommunicatie geldt wel een verplichting om aan een dergelijk verzoek tegemoet te komen. Het verzoek dient dan wel betrekking te hebben op (telecom-)verkeers- en NAW gegevens. Een dergelijk verzoek valt echter onder de bijzondere bevoegdheden, zie artikelen 28 en 29 WIV 2002.

overeenkomsten namens een bedrijf aan te gaan.[106] Dit zijn alle specifieke doelstellingen voor de verwerking van persoonsgegevens. Maar deze gegevens kunnen ook interessant zijn voor een veiligheidsdienst zoals de AIVD.

Een belangrijk uitgangspunt van regelgeving omtrent databescherming (zie de Wet Bescherming Persoonsgegevens) is echter doelbinding: persoonsgegevens mogen alleen worden verwerkt ten behoeve van het doel waarvoor zij zijn verkregen.[107] Indien de AIVD een bedrijf benadert met het verzoek bepaalde gegevens te verstrekken (de algemene bevoegdheid van artikel 17 WIV 2002), dan is het aan de bevraagde hier al dan niet op in te gaan. Maar als hij besluit persoonsgegevens aan de dienst te verstrekken, dan kan hij op problemen stuiten indien de privacywetgeving waar hij onder valt geen uitzonderingsbepaling met betrekking tot de doelbinding kent, in casu voor verstrekkingen in het kader van de bescherming van de nationale veiligheid. Artikel 43 sub a WBP biedt hierom een aantal uitzonderingen op de doelbindingseis, waaronder 'de veiligheid van de staat'. Het beschermen van de veiligheid van de staat is één van de taken van de AIVD. Maar de dienst heeft ook tot taak het beschermen van de democratische rechtsorde of het beschermen van andere gewichtige belangen dan de veiligheid van de staat (zoals economisch welzijn). Het zou bij een strikte lezing volgens de WBP dus mogelijk zijn om geen gehoor te geven aan het verzoek van de AIVD indien het één van de andere taken dan veiligheid van de staat betreft.[108] Nu kan de bescherming van de democratische rechtsorde in veel gevallen onder deze laatste categorie worden geschaard. Zo is er in geval van terrorisme duidelijk sprake van bescherming van de rechten van anderen, namelijk het recht op leven zoals neergelegd in artikel 2 EVRM. Er zijn echter ook gevallen denkbaar die niet onder deze categorie vallen, zoals corruptie van een hoge ambtenaar. Hierbij hoeft geen sprake te zijn van een bedreiging van de veiligheid van de staat, maar dit kan in bepaalde gevallen wel weer een bedreiging van de democratische rechtsorde opleveren. Er is echter geen recht of vrijheid van anderen in het geding. In dit geval kan iemand op basis van de WBP strikt genomen geen gehoor geven aan het verzoek van de AIVD. Voor deze gevallen biedt het derde lid van artikel 17 WIV 2002 een oplossing. Kort gezegd stelt dit lid dat de voorschriften die gelden voor een verstrekking in het algemeen niet van toepassing zijn op verstrekkingen van persoonsgegevens aan de AIVD op basis van een artikel 17 verzoek. Er zijn dus geen juridische belemmeringen voor een dergelijke verstrekking. Een bijkomend doel van de bepaling is overigens de verstrekker te ontheffen van enige protocolplicht. Op deze manier wordt voorkomen dat degene wiens persoonsgegevens aan de dienst worden verstrekt op de hoogte geraakt van AIVD-activiteiten. De houder van de persoonsgegevens behoeft daarnaast aan een eventuele toezichthouder geen verstrekking aan de AIVD te melden: dit valt onder de ontheffing die artikel 17 lid 3 WIV verleent.[109]

Mensen die op basis van artikel 17 WIV 2002 informatie aan de dienst verstrekken worden informanten genoemd. Onder 'informant' verstaat de WIV: "*de natuurlijke persoon die door zijn hoedanigheid of door de positie waarin hij verkeert, over gegevens beschikt of kan beschikken die voor een goede taakuitoefening door de dienst van belang kan zijn*" (Van der Bel et al. 2009: 272-273). Zoals later nog zal

[106] Artikel 2 sub a Handelsregisterwet.
[107] Zie bijvoorbeeld artikel 9 lid 1 WBP.
[108] De MvT geeft hierover trouwens geen uitsluitsel en gaat slechts in op één van de andere uitzonderingen op de doelbinding, namelijk de bescherming van de betrokkene of van de rechten en vrijheden van anderen.
[109] *Kamerstukken II,* 1997/98, 25 877, nr. 3, p. 23-24. Zie ook: Van der Bel et al. (2009: 267-268).

blijken, lijkt de informant van de WIV in veel opzichten op de informant van de CIE, met dien verstande dat artikel 17 WIV 2002 een expliciete algemene bevoegdheid is. In subsectie 3.3.6 behandelen wij de figuur van de AIVD-informant.

Nu biedt artikel 17 WIV 2002 de dienst weliswaar een algemene informatiebevoegdheid, maar het gehoor geven aan een dergelijk artikel 17 verzoek vindt plaats op basis van vrijwilligheid. De informatie die ermee verzameld wordt, zijn persoonsgegevens die door anderen worden geregistreerd. Het ligt voor de hand dat de AIVD ook andere informatie wil verkrijgen, informatie die niet als persoonsgegevens in databanken is geregistreerd. Zo zal hij de inhoud van telefoongesprekken willen weten, brief- of email correspondentie willen lezen en bij vergaderingen van bepaalde (staatsgevaarlijke) organisaties aanwezig willen zijn. Voor het verzamelen van dit soort informatie heeft de dienst zogenoemde 'bijzondere bevoegdheden', die in de volgende sectie kort worden behandeld.

3.3.2 De bijzondere bevoegdheden

De bijzondere bevoegdheden van de AIVD staan geregeld in de artikelen 20 tot en met 30 van de WIV 2002. Voorbeelden zijn het volgen en observeren van subjecten en de inzet van agenten (respectievelijk artikel 20 en 21 WIV 2002).

Bij onze inhoudelijke behandeling van de bevoegdheden van de AIVD staan met name de bevoegdheden centraal die van belang kunnen zijn bij de samenwerking met de politie in het algemeen en de CIE in het bijzonder. Het gaat dan om de methoden die bekend staan onder de noemer 'HUMINT', oftewel '*human intelligence*'. Voordat de verschillende aspecten van de HUMINT aan de orde komen, maken we eerst een aantal algemene opmerkingen over het toepassen van de bijzondere inlichtingenmiddelen.

Zo moet de toepassing van de bijzondere inlichtingenmiddelen altijd worden getoetst aan subsidiariteit en proportionaliteit. De algemene voorwaarde is dat bijzondere bevoegdheden slechts mogen worden uitgeoefend indien dit *noodzakelijk* is voor de goede uitvoering van de taken bedoeld in artikel 6 lid 2, sub a en d WIV 2002, aldus artikel 18 WIV 2002. Dit is een belangrijke beperking voor de toepassing van de AIVD bevoegdheden: bijzondere bevoegdheden kan de AIVD alleen in het kader van de A of de D-taak inzetten. Het is dus niet mogelijk om in het kader van een veiligheidsonderzoek een telefoontap in te zetten op een te screenen subject. In de volgende subsecties komen de subsidiariteit en proportionaliteit aan bod.

3.3.3 Subsidiariteit

De subsidiariteitseis bij de toepassing van de bijzondere inlichtingenmiddelen wordt uitgewerkt in artikel 31 WIV 2002 en houdt in dat de toepassing is geoorloofd indien de daarmee beoogde verzameling van gegevens niet of niet tijdig kan geschieden door de raadpleging van open bronnen of van bronnen waarvoor aan de dienst een recht op kennisneming van de betreffende gegevens is verleend (lid 1). Dit is onder meer van belang met betrekking tot de verhouding tussen de politie en de AIVD. Zo heeft de dienst een dergelijk recht op kennisneming van politiegegevens op basis van artikel 62 WIV 2002 (zie subsectie 4.5.3). Of bepaalde informatie al dan niet tijdig kan worden verzameld, hangt af van welke tijdsdruk bestaat voor het wegnemen van een bepaalde dreiging (Van der Bel et al. 2009: 271). Het ligt voor de hand dat bij een dreiging van terroristische aanslagen de tijdsdruk hoger zal zijn dan bijvoorbeeld bij een onderzoek naar aanwezigen op een vergadering van de communistische partij.

Onder het criterium 'niet of niet tijdig' valt ook de situatie van twijfel omtrent de juistheid of volledigheid van de gegevens die de dienst heeft verkregen. De subsidiariteitstoets heeft zowel een algemeen aspect (is de informatie aanwezig en tijdig te verkrijgen) en een inhoudelijk aspect (is de informatie juist en volledig). In het hierboven genoemde geval van het doen van onderzoek naar wie er aanwezig zijn geweest bij een vergadering van de communistische partij kan het zijn dat, indien er een vergadercentrum of iets dergelijks is gehuurd, een aanwezigheidslijst wordt opgevraagd bij het centrum (indien een dergelijke lijst wordt bijgehouden). Als er redenen bestaan om aan te nemen dat er mensen aanwezig zullen zijn die niet op zo'n lijst voorkomen, dan kan dat een reden zijn om alsnog een bijzondere bevoegdheid in te zetten. De AIVD mag dus eerst overgaan tot het verzamelen van een grote hoeveelheid (politie)gegevens omtrent persoon x om daarna, als er twijfel bestaat omtrent de juistheid en volledigheid van de informatie, alsnog over te gaan tot het toepassen van één van de bijzondere inlichtingenmiddelen. Een dergelijke situatie van twijfel lijkt zich trouwens al snel voor te doen: er is immers altijd wel iets dat je mogelijk niet weet (onvolledige informatie) of informatie is in potentie onjuist. De vraag lijkt dan ook gerechtvaardigd of er inderdaad wel een subsidiariteitstoets plaatsvindt. Het gaat echter te ver om deze problematiek in dit onderzoek te behandelen. Naast de subsidiariteit dient de AIVD bij de inzet van bijzondere inlichtingenmiddelen ook rekening te houden met de proportionaliteit.

3.3.4 Proportionaliteit

Als is besloten om een bijzondere bevoegdheid in te zetten, dient de dienst te kiezen voor de minst ingrijpende bevoegdheid: "*slechts die bevoegdheid wordt toegepast die gelet op de omstandigheden van het geval, waaronder de ernst van de bedreiging van de door de dienst te beschermen belangen, mede in vergelijking met andere beschikbare bevoegdheden, voor de betrokkene het minste nadeel oplevert*" (Van der Bel et al. 2009: 272).[110] De proportionaliteitseis valt uiteen in een negatief en een positief geformuleerde voorwaarde. De toepassing van een bijzondere bevoegdheid mag voor de betrokkene in vergelijking met het doel dat met de toepassing beoogd is, geen onevenredig nadeel opleveren. Ook de concrete uitoefening van de bevoegdheid dient evenredig te zijn aan het daarmee beoogde doel (Van der Bel 2009: 271). Indien het doel waartoe de bevoegdheid wordt uitgeoefend is bereikt, of als er kan worden volstaan met de uitoefening van een andere, minder ingrijpende bevoegdheid, dient de uitoefening van de bijzondere bevoegdheid onmiddellijk te worden gestaakt. In dit opzicht verwijzen we naar artikel 8 EVRM: een inbreuk op de persoonlijke levenssfeer van burgers is toegestaan indien deze *noodzakelijk* is in een democratische samenleving.

3.3.5 Praktijk en procedures

Nu klinkt het bovenstaande op zichzelf logisch: de AIVD kan niet zomaar bepaalde middelen inzetten, maar moet hiervoor redenen hebben en is bij het beslissen om al dan niet een bijzonder middel in te zetten, gebonden aan eisen van subsidiariteit en proportionaliteit. Maar welke weg dient de dienst te bewandelen voordat besloten kan worden tot de inzet van dergelijke middelen? Met andere woorden: hoe bepaalt de

[110] De proportionaliteittoets vloeit voort uit artikel 31 lid 2 WIV 2002, zie ook *Kamerstukken II*, 1997/98, 25 877, nr. 3, p. 52.

dienst met het oog op subsidiariteit en proportionaliteit welke middelen worden toegepast en welke niet?

Bij het starten van een onderzoek bepaalt het onderzoeksteam welke informatie nodig is. Om te beginnen wordt er bijvoorbeeld een open-bronnen onderzoek verricht en kijkt het team welke informatie hij in de eigen systemen kan vinden en welke informatie elders in open bronnen, zoals het internet, opgeslagen ligt. Als er dan nog informatievragen open staan, formuleert het team vervolgens welke informatie hij nog nodig heeft en daarna stelt een team dat belast is met de inzet van de bijzondere inlichtingenmiddelen vast welke middelen het beste kunnen worden ingezet en in welke samenstelling om een antwoord op de vraag te krijgen. Bij deze overweging speelt, naast de bovengenoemde subsidiariteit- en proportionaliteitsvraagstukken, ook de beschikbare capaciteit een belangrijke rol (Commissie Havermans 2004: 124).[111]

Bij het nemen van beslissingen omtrent de toepassing van bijzondere inlichtingenmiddelen is de aan de beslissing voorafgaande dreigingsanalyse van belang. Welke normen het toetsingskader vormen is echter niet te zeggen: dit hangt af van het specifieke geval. De normen moeten immers in een veelvoud van situaties toepasbaar zijn. Voorts is er ook geen rangorde tussen de bevoegdheden aan te brengen.[112]

Naast een toetsingskader met betrekking tot subsidiariteit en proportionaliteit spelen afwegingen omtrent efficiency en effectiviteit een rol.[113] In de praktijk zullen met name deze laatste overwegingen van belang zijn. Iedere bevoegdheid ziet namelijk op het verkrijgen van een specifieke soort informatie. Een telefoontap levert de inhoud van telefoongesprekken op, en het openmaken van post levert schriftelijke correspondentie op. De keuze tussen welke van deze twee uiteindelijk toepassing zal vinden is afhankelijk van de concrete zaak. Iemand die mogelijk betrokken is bij terroristische activiteiten en die telefonisch contact onderhoudt met buitenlandse leden van een terroristisch netwerk, zal getapt worden. De keuze voor het openmaken van de post aan zijn moeder in het thuisland ligt minder voor de hand, niet omdat dit ingrijpender is, maar met name omdat dit weinig zal opleveren dat voor de dienst interessant is.[114] Let wel: ook de ernst van de dreiging is een onderdeel van het toetsingskader. Het is goed denkbaar en waarschijnlijk dat bij een mogelijke terroristische aanslag vrijwel alle bevoegdheden die de dienst tot zijn beschikking heeft, worden ingezet.

Indien men vervolgens kiest voor het toepassen van een bijzonder inlichtingenmiddel, dient de voor de betrokkene minst ingrijpende bevoegdheid te worden toegepast (proportionaliteit). Welk middel dit precies is, hangt af van de omstandigheden van het geval. Onder de omstandigheden van het geval valt ook de ernst van de dreiging. Terrorisme zal sneller nopen tot het inzetten van een zwaarder middel dan lidmaatschap van een communistische partij (maar ook dit kan onder bepaalde omstandigheden van het geval afhangen).

Van de toepassing van een bijzonder inlichtingenmiddel dient volgens artikel 33 WIV 2002 een schriftelijk verslag te worden opgemaakt. Dit gebeurt ter controle

---

[111] De Commissie Havermans noemt nog de Directie Bijzondere Inlichtingenmiddelen, maar zoals in sectie 4.1 reeds is aangegeven, bestaat deze directie niet meer.

[112] *Kamerstukken II*, 1997/98, 25877, nr. 3, p. 51.

[113] *Kamerstukken II*, 1997/98, 25 877, nr. 3, p. 51-52.

[114] Proportionaliteit en effectiviteit zullen vaak door elkaar heen lopen. Het is disproportioneel om iemand te tappen als je redelijkerwijze kunt vermoeden dat de tap niet iets relevant zal opleveren. Maar ook hier geldt dat een dienst vooraf nooit kan weten wat ze niet weten.

en verantwoording achteraf, niet alleen intern maar ook naar, bijvoorbeeld, een Commissie van Toezicht op de Inlichtingen- en veiligheidsdiensten (zie ook subsectie 3.7.2).

Eén van belangrijkste bijzondere inlichtingenmiddelen waar de AIVD gebruik van maakt, is de agent. Dit is het onderwerp van de volgende subsectie.

3.3.6 HUMINT: het runnen van agenten door de AIVD

Het belangrijkste bijzondere inlichtingenmiddel in het kader van ons onderzoek is de agent: de natuurlijke persoon die, al dan niet onder dekmantel van een aangenomen identiteit of hoedanigheid, onder verantwoordelijkheid en onder aansturing van de dienst wordt ingezet om gericht informatie te verzamelen of het treffen van bepaalde maatregelen te bevorderen ter bescherming van door de dienst te behartigen belangen (artikel 21 lid 1 sub a WIV 2002).[115] Een andere naam voor deze persoon spreekt wellicht meer tot de verbeelding: de spion. In het inlichtingenjargon betekent de term 'agent' dus iets fundamenteel anders dan in de politiewereld: het is geen politieambtenaar ('diender'). Het is ook belangrijk om te realiseren dat er een belangrijk verschil is tussen de figuur van de agent en de figuur van de informant. De agent wordt door de AIVD gestuurd en staat in dat opzicht onder controle van de dienst.[116] De informant heeft de beschikking over voor de AIVD interessante informatie, maar wordt bij de verzameling van die informatie niet gestuurd. Beide figuren verrichten de medewerking echter op basis van vrijwilligheid. Voor de agent is de juridische grondslag artikel 21 lid 1 sub a WIV 2002, voor de informant artikel 17 WIV 2002 (Van der Bel et al. 2009: 272).

Soms is een agent een medewerker van de AIVD die een veiligheidsonderzoek heeft ondergaan en op zijn geschiktheid is getest om bijvoorbeeld in een netwerk te infiltreren. Het kan echter ook zijn dat iemand die geen medewerker van de dienst is, als agent wordt ingezet. Ten aanzien van deze laatste categorie personen worden de middelen die de AIVD tot zijn beschikking heeft ingezet om een oordeel over de betrouwbaarheid van de persoon te verkrijgen. Het is overigens mogelijk dat er gedurende een bepaalde tijd wel met iemand wordt gewerkt zonder dat er sturing plaatsvindt.[117] Iemand kan bijvoorbeeld eerst een tijd lang als informant fungeren en later, als de verstrekte informatie en de betreffende informant zelf betrouwbaar blijken, als agent worden ingezet.

Bij het runnen van agenten is specifieke toestemming nodig van de Minister van Binnenlandse Zaken of het gemandateerde hoofd van de AIVD[118], hetgeen geen vereiste is voor het runnen van informanten. In de praktijk hanteert de AIVD dezelfde procedure voor het runnen van agenten en informanten, wat betekent dat voor beiden vooraf toestemming wordt gevraagd (Van der Bel et al. 2009: 260). Op deze manier heeft de AIVD het overzicht over het totale aantal bronnen. Daarnaast is het van tevoren vaak niet goed in te schatten of iemand agent of informant is. Het is mogelijk dat iemand die in eerste instantie wordt aangemerkt als informant, op een later moment meer sturing bij het verzamelen van informatie vereist en daarmee een agent

[115] Dit artikel regelt ook de oprichting en inzet van rechtspersonen ter ondersteuning van operationele activiteiten: de zogenoemde 'frontstores'.
[116] *Kamerstukken II*, 1999/2000, 25 877, nr. 8, p. 59.
[117] Brief minister BZK, *Kamerstukken II*, 1999/2000, 25 877, nr. 59, p. 9.
[118] In een aantal gevallen is besloten dat slechts de minister toestemming kan verlenen; dus ook niet in mandaat door het hoofd van de AIVD. Het gaat dan bijvoorbeeld om de opdracht aan bestuursorganen om medewerking te verlenen bij het creëren van een pseudo-identiteit (artikel 21 lid 2 WIV 2002).

wordt. Door in de procedure voor beide figuren vooraf toestemming te vragen, voorkomt de AIVD dat er inschattingsfouten worden gemaakt en een agent onterecht als informant wordt aangemerkt, waarmee het werken met deze agent onrechtmatig kan zijn. De vraag die nu rijst is: wat doet een agent?

3.3.7 Wat doet een agent?

We hebben in de vorige subsectie al de juridische definitie van een agent gegeven. In deze subsectie staan we kort stil bij wat een agent doet. De primaire taak van de agent is om gericht informatie te verzamelen. Deze informatie kan worden verstrekt aan bijvoorbeeld politie en justitie, die vervolgens maatregelen kunnen treffen. Maar soms is hier geen tijd voor. In die specifieke gevallen heeft de agent de mogelijkheid om bepaalde maatregelen te bevorderen of te treffen ter bescherming van door de dienst te behartigen belangen. Het doel van deze maatregelen is te voorkomen dat risico's van schendingen van een in de WIV 2002 genoemd belang ook werkelijkheid worden. Deze maatregelen zullen worden bevorderd of getroffen indien geen betere bestuurlijke maatregelen mogelijk zijn of indien deze latere acties naar verwachting gepaard zullen gaan met onevenredige inspanningen en risico's voor de in het geding zijnde belangen.[119] Voorbeelden van maatregelen zijn het verspreiden van desinformatie of het frustreren van voorgenomen gewelddadige acties.[120] Dit kan op heel veel verschillende manieren. Hieronder geven we een voorbeeld dat tijdens onze interviews werd genoemd.

"*Je komt bijvoorbeeld 10 vervalste paspoorten tegen. Die kunnen voor 'normale' strafbare feiten worden gebruikt, maar ook voor terroristische aanslagen. Je wilt als dienst niet dat die dingen worden gebruikt, maar je kan ook niet naar andere partijen om die te laten ingrijpen* (omdat je dan de informatiepositie kwijt bent, opmerking auteur). *Wat doe je dan? Je moet wel handelen. Wat we in zo'n geval bijvoorbeeld kunnen doen is de paspoorten behandelen met een bepaalde soort chemicaliën die de paspoorten na een bepaalde tijd onbruikbaar maken."* (voormalig) medewerker AIVD (A), januari 2008.

Een belangrijk verschil met verstoringacties van de politie is dat de inmenging van de dienst zoveel mogelijk verborgen blijft. Het is dus niet de bedoeling dat bekend wordt dat een bepaalde actie door de AIVD is verricht: het is en blijft immers een geheime dienst.

Agenten worden begeleid door zogenoemde 'operateurs' (in CIE-termen 'runners'). Van ontmoetingen tussen de operateur en de agent wordt een operatierapport opgemaakt. Hierin wordt de gehele ontmoeting beschreven, inclusief gegevens over de agent zelf. Het operatierapport geeft dus ook inzicht in de identiteit van de agent en is daarom alleen bekend bij een kleine kring medewerkers van de dienst. Naast het operatierapport wordt er ook een informatierapport opgesteld. Hierin staat de informatie die van waarde is voor de taakuitoefening door de dienst, zonder dat de persoonlijke gegevens van de agent worden prijsgegeven. In voorkomende gevallen wordt er op basis van het informatierapport een ambtsbericht uitgegeven (Van der Bel et al. 2009: 274. Zie ook subsectie 3.4.2. voor de inhoudelijke behandeling van de ambtsberichtprocedure).

[119] *Kamerstukken II*, 1997/98, 25 877, nr. 3, p. 34.
[120] *Kamerstukken II*, 1999/2000, 25 877, nr. 8, p. 61.

3.3.8 De agent en strafbare feiten

Waarom is de figuur van de agent nu specifiek voor dit onderzoek van belang? Agenten begeven zich vaak in een omgeving waarin strafbare feiten worden gepleegd. Om niet ontmaskerd te worden, dient de agent geloofwaardig te zijn en dit betekent dikwijls dat hij moet participeren in het plegen van de strafbare feiten: "*hij dient zich met andere woorden zoveel als mogelijk is te conformeren aan het in de betreffende organisatie geldend groepsgedrag. In voorkomende gevallen kan zich daarbij de situatie voordoen dat door betrokkene medewerking moet worden verleend aan het plegen van strafbare feiten dan wel strafbare feiten moeten worden gepleegd.*"[121] Het conformeren aan de groep is zowel van belang voor de veiligheid van de agent als voor het winnen van vertrouwen van zijn omgeving. In principe is de agent in dergelijke gevallen straffeloos, mits aan een aantal voorwaarden is voldaan. Artikel 21 lid 3 WIV 2002 stelt namelijk dat een agent bij instructie van de dienst kan worden belast met het verrichten van handelingen die als gevolg kunnen hebben dat medewerking wordt verleend aan het plegen van een strafbaar feit, dan wel daadwerkelijk een strafbaar feit wordt gepleegd. Aan de agent wordt in de instructie aangegeven onder welke omstandigheden de mogelijk strafbare handelingen mogen worden verricht en de wijze waarop aan de instructie (en de daarin genoemde mogelijke strafbare feiten) uitvoering dient te worden gegeven, voor zover dat bij het geven van de instructie is te voorzien. Dit volgt uit de leden 3 en 5 van artikel 21 WIV 2002. Met de laatste zinsnede geeft de wetgever aan dat het mogelijk is dat een agent in een situatie terecht komt waarin hij strafbare feiten moet (mede)plegen die niet in de instructie voorkomen. De vraag is of de agent dan ook straffeloos is. De instructie is namelijk een bevoegd gegeven ambtelijk bevel waardoor artikel 43 WvSr (rechtvaardigingsgrond) van toepassing is.[122] Maar indien de agent strafbare handelingen verricht die niet in de instructie worden genoemd, dan zou deze rechtvaardigingsgrond wegvallen. Het gaat in het kader van dit onderzoek te ver om de rechtvaardigingsgronden die dan van toepassing zijn te behandelen, maar het is goed denkbaar dat agenten in situaties terechtkomen van overmacht. Immers, als het niet plegen van een strafbaar feit tot gevolg heeft dat de agent wordt ontmaskerd en vervolgens levensgevaar loopt, dan kun je al snel van overmacht spreken. In het algemeen zal de agent dus redelijk straffeloos kunnen opereren.[123] De instructie wordt overigens schriftelijk vastgelegd, aldus lid 6 van hetzelfde artikel. Daarnaast bepaalt lid 4 dat de agent bij de uitvoering van de instructie door zijn optreden een persoon niet mag brengen tot ander handelen betreffende het beramen of plegen van strafbare feiten, dan waarop diens opzet reeds tevoren was gericht. Met andere woorden: van

[121] *Kamerstukken II*, 1997/98, 25 877, nr. 3, p. 32.

[122] *Kamerstukken II*, 1997/98, 25 877, nr. 3, p. 33. Alhoewel de agent materieel straffeloos is, kan hij formeel geen beroep doen op de rechtvaardigingsgrond van artikel 43 WvSr omdat hij gehouden is aan zijn geheimhoudingsplicht (zie voor de geheimhouding ook subsectie 3.4.2). Door zich op artikel 43 WvSr te beroepen, kan de agent vervolgd worden voor het schenden van de geheimhoudingsplicht, en loopt hij een mogelijk veiligheidsrisico van de zijde van degenen over wie hij informatie heeft verzameld (Van der Bel et al. 2009: 277).

[123] De wetgever heeft er voor gekozen geen limitatieve opsomming van strafbare feiten te geven die in een dergelijke instructie kunnen worden opgenomen. Dit zou de organisaties waarin agenten infiltreren een soort checklist geven van strafbare feiten om de (on)betrouwbaarheid van de betrokkene vast te stellen. Een categoriale aanduiding van een bepaald soort delict lijkt de wetgever ook onwenselijk, deels vanwege dezelfde problemen als bij de lijst, maar ook omdat '*een categoriale aanduiding met betrekking tot de beantwoording van de zo belangrijke vraag of iemand al dan niet strafbaar is, onvoldoende rechtszekerheid biedt*' (*Kamerstukken II*, 1997/98, 25 877, nr. 3, p, 34.

uitlokking mag ook door agenten van de AIVD geen sprake zijn (het Tallon-criterium).

Het OM heeft een adviserende rol bij de afweging of, en zo ja, welke strafbare feiten een agent mag plegen.[124] Deze raadplegende rol van het OM wordt in de praktijk ingevuld door de officier van justitie van het Landelijk Parket belast met terrorismebestrijding. Deze officier van justitie zal in een vroeg stadium geïnformeerd dienen te worden over de instructie en inzet van een agent.

In het kader van dit onderzoek is het niet zozeer van belang dat de agent straffeloos strafbare feiten mag plegen (voor zover deze passen in de strekking van de instructie). Door de mogelijkheid dat de agent betrokken kan zijn bij het plegen van strafbare feiten, is de kans groot dat hij of zij op een gegeven moment in beeld komt bij de politie als verdachte. Dit is voor de dienst om meerdere redenen nadelig. Zo is er het algemene risico van het uitlekken van de identiteit van agenten. Dit is een algemeen veiligheidsrisico voor de agent, maar het verschaft de politie ook mogelijk inzicht in de inlichtingentrajecten van de dienst en diens informatiepositie. De afscherming van de identiteit van de agent (en trouwens ook de informant) en de informatiepositie heeft voor een veiligheidsdienst absoluut de hoogste prioriteit, zie ook hoofdstuk twee.

Voorts is er het algemene risico van een eventuele aanhouding van de agent. Naast het risico dat de identiteit van de agent bekend wordt in de strafprocedure omdat hij een beroep zal doen op een rechtvaardigingsgrond, raakt de dienst ook nog eens zijn informatiepositie kwijt. Met het naar voren schuiven van het strafrecht is in de laatste jaren de kans steeds groter dat agenten van de AIVD onderwerp van politieonderzoek worden. Dit maakt het voor de AIVD steeds belangrijker om precies te weten welke onderzoeken de politie draait.

Als de informatie is verzameld, volgt de fase van het verwerken. Ook hiervoor gelden bepaalde regels.

3.4 Informatieverwerking

Gegevensverwerking wordt gedefinieerd in artikel 1 sub f WIV 2002 als: "*(…) elke handeling of elk geheel van handelingen met betrekking tot gegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van ter beschikking stelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens*".[125] Deze definitie ziet zowel op de handmatig gevoerde als de geautomatiseerde gegevensverwerking en is niet beperkt tot persoonsgegevens.[126] Dus ook de met de hand bijgehouden operatieverslagen van de operateurs vallen onder het regime van de WIV 2002. Gegevensverwerking omvat dus vrijwel alles wat een dienst doet: het is het "primaire bedrijfsproces" van de AIVD.[127] Algemene regels voor gegevensverwerking staan in hoofdstuk 3 van de wet. Artikel 12 stelt onder meer

[124] *Kamerstukken II*, 1997/98, 25 877, nr. 3, p. 34. Zie Van der Bel et al. (2009: 276-277).

[125] Bij de definitie van gegevensverwerking is aangesloten bij de door het Europees Parlement en de Raad van Ministers van de Europese Gemeenschappen vastgestelde richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens van 24 oktober 1995 (95/46/EG; PbEG l 281 van 23 november 1995) en de Wet Bescherming Persoonsgegevens.

[126] *Kamerstukken II*, 1997/98, 25 877, nr. 3, p. 17-18. Hetgeen anders is bij de Wet Politiegegevens: deze wet heeft wel nadrukkelijk alleen betrekking op de verwerking van persoonsgegevens.

[127] *Kamerstukken II*, 1997/98, 25 877, nr. 3, p. 16.

in lid 1 dat de diensten bevoegd zijn tot het verwerken van gegevens met inachtneming van de eisen die daaraan bij of krachtens de WIV 2002 (of de Wet veiligheidsonderzoeken) zijn gesteld. Verder stelt lid 2 dat gegevensverwerking slechts plaats kan vinden met een bepaald doel en slechts indien dat noodzakelijk is voor een goede uitvoering van de WIV 2002. Lid 4 stelt vervolgens dat verwerkte gegevens dienen te zijn voorzien van een aanduiding omtrent de mate van betrouwbaarheid danwel een verwijzing naar het document of de bron waaraan de gegevens zijn ontleend. Wat er precies met de verzamelde gegevens gebeurt, is geheim. De AIVD houdt informatie omtrent zijn methoden van werken geheim, omdat als deze bekend zouden worden, de dienst daar nadelen van ondervindt.

Uit artikel 1 sub f WIV 2002 volgt overigens ook dat het verstrekken van gegevens juridisch moet worden gezien als een vorm van gegevensverwerking. Dit leidt wellicht tot wat terminologische verwarring, omdat verwerking ook kan worden gezien als *throughput*. De verstrekking van gegevens is dan de *output*. Wij behandelen de verstrekking van gegevens apart in de volgende subsecties (3.4.1 en 3.4.2).

De belangrijkste vorm van verwerking van gegevens door de AIVD is in het kader van dit onderzoek de verstrekking van informatie aan politie en justitie. Wij beginnen onze behandeling van de verstrekkingsmodaliteiten echter bij de interne gegevensverstrekking (3.4.1). Belangrijker dan de interne gegevensverstrekking zijn de verstrekkingen aan externe partijen. De bepalingen van de WIV 2002 die de externe gegevensverstrekking reguleren, bepalen een belangrijk deel van de formele verhouding tussen de AIVD en de CIE. Met betrekking tot de verstrekking van informatie aan externe partijen, politie en justitie daarbij inbegrepen, kent de dienst namelijk een zogenoemd 'gesloten stelsel'. Dit behandelen wij in subsectie 3.4.2.

3.4.1 Interne gegevensverstrekking

Binnen de AIVD geldt het uitgangspunt van '*need to know*'. Dit uitgangspunt komt tot uitdrukking in artikel 35 WIV 2002. Door de dienst verwerkte gegevens mogen alleen binnen de dienst worden verstrekt als dat noodzakelijk is voor de goede taakuitvoering van de betreffende ambtenaar. Aan het *need to know* uitgangspunt liggen twee overwegingen ten grondslag. De eerste overweging is dat de persoonlijke levenssfeer van de betrokkene zo min mogelijk geschonden wordt.[128] De gegevens waarover de AIVD beschikt zijn op zichzelf al privacygevoelig en dit geldt sterker omdat de gegevens door de dienst worden verwerkt. Het feit dat iemand een AIVD-subject is, dat wil zeggen dat de AIVD gegevens omtrent deze persoon verzamelt en verwerkt, is op zichzelf al gevoelige informatie. Daarom probeert de dienst de gegevensverspreiding intern zo beperkt mogelijk te houden: alleen de ambtenaar die de gegevens nodig heeft voor een goede uitvoering van zijn taak mag de gegevens verstrekt krijgen. Privacybescherming is dus één reden voor *need to know*.

De tweede overweging voor *need to know* is gelegen in het belang van veiligheid voor de dienst. Door informatie beperkt intern te verstrekken, loopt een veiligheidsdienst minder schade op indien er sprake is van een 'lek'; een ambtenaar van de dienst die ook voor vijandelijke diensten of organisaties werkt. Immers, de betreffende ambtenaar weet alleen wat voor de goede uitvoering van zijn specifieke

[128] *Kamerstukken II*, 1997/98, 25 877, nr. 3, p. 54. Zie ook Van der Bel et al. (2009: 296).

taak van belang is. Over informatie van andere teams kan hij niet beschikken. *Need to know* is dus met name een veiligheidsmaatregel.[129]

In de praktijk geldt het uitgangspunt van *need to know* met name tussen teams. Volgens oud-medewerkers van AIVD is er binnen de teams zelf een hoge mate van openheid en wordt informatie vrijelijk gedeeld.[130] Dit is verklaarbaar en te verdedigen omdat de leden van het team allemaal dezelfde taak hebben en daarom de beschikking moeten hebben over dezelfde informatie. De compartimentalisatie binnen de AIVD werkt aldus niet alleen op directieniveau, maar ook binnen de directies tussen de verschillende teams. Op deze manier wordt getracht de schade uit een eventueel lek zoveel mogelijk te beperken.

Onder de noemer 'interne gegevensverstrekking' valt overigens ook de verstrekking aan artikel-60 ambtenaren, zoals medewerkers van de Regionale Inlichtingen Dienst (RID) en de Contra-Terrorisme Informatie Box (CT-Infobox).

3.4.2 De externe gegevensverstrekking: gesloten verstrekkingsregime

Eén van de belangrijkste partners van de AIVD is de politie. De politie kan immers in tegenstelling tot de dienst wel overgaan tot aanhouding van individuen, mits er aan bepaalde criteria is voldaan. De dienst heeft overigens geen zeggenschap over de politie, hij kan dus geen bevel geven om een opsporingsonderzoek te starten of te stoppen.[131] De politie moet informatie krijgen van de AIVD waarna zij tot actie kan overgaan (bijvoorbeeld een opsporingsonderzoek of het verstoren van activiteiten die een bedreiging van de nationale veiligheid vormen). Deze informatieverstrekking is aan strenge regels gebonden, die de formele verhouding tussen beide organisaties bepalen.

Voor de AIVD geldt een gesloten verstrekkingsregime. Dit houdt in dat verstrekking van door de AIVD verwerkte gegevens slechts plaats dient te vinden indien hiervoor een expliciete wettelijke basis bestaat (Van der Bel et al. 2009: 296).[132] De basis voor externe verstrekkingen is artikel 36 WIV 2002: "*de diensten zijn in het kader van een goede taakuitvoering bevoegd om omtrent door of ten behoeve van de dienst verwerkte gegevens mededeling te doen (…)*". Vervolgens somt het artikel specifiek op aan wie kan worden verstrekt: onze ministers wie deze aangaan, andere bestuursorganen wie deze aangaan, andere personen of instanties wie deze aangaan en daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen.

De zinsnede "*doen van een mededeling omtrent een door of ten behoeve van de dienst verwerkte gegevens*" impliceert dat het gaat om op enigerlei wijze door de dienst bewerkte gegevens, en niet om de oorspronkelijk aan de mededeling ten grondslag liggende gegevens (Van der Bel et al. 2009: 296). Als ook tapuitwerkingen en operatierapporten worden verstrekt, komen mogelijk de bronnen en de modus operandi van de dienst in gevaar. Het verstrekken van dergelijke gegevens is in strijd met de geheimhoudingsplicht uit artikel 15 WIV 2002.

---

[129] *Ibid*.

[130] Interview (voormalig) medewerker AIVD (A), januari 2008.

[131] Het bevoegd gezag van de politie is het Openbaar Ministerie, zie artikel 2 Politiewet 1993 jo. artikel 13 Politiewet 1993.

[132] Zie ook: Commissie van Toezicht betreffende de Inlichtingen- en veiligheidsdiensten, *Toezichtsrapport 9a: Inzake het onderzoek van de Commissie van Toezicht naar de door de AIVD uitgebrachte ambtsberichten in de periode van januari 2004 tot oktober 2005*, 31 mei 2006, te downloaden van: http://www.ctivd.nl/, gezien op 23 november 2009.

Wij behandelen in deze subsectie verder (A) artikel 15 WIV 2002, (B) de modaliteit van verstrekkingen, te weten de ambtsberichten, en (C) de mogelijkheid van parallelonderzoeken.

(A) Artikel 15 WIV 2002: geheimhouding

Artikel 15 WIV 2002 is de algemene geheimhoudingsbepaling van de WIV. Het draagt het hoofd van de dienst op om zorg te dragen voor enerzijds de geheimhouding van gegevens en de bronnen waaruit deze gegevens afkomstig zijn en anderzijds de veiligheid van de personen met wier medewerking gegevens worden verzameld (agenten en informanten). De verplichting tot het beschermen van de technische bronnen en de veiligheid van de menselijke bronnen zijn voor de dienst absoluut.[133] De oorspronkelijk aan de mededeling ten grondslag liggende gegevens worden als hoofdregel niet verstrekt indien de lange termijn doelstellingen van de dienst zich daartegen verzetten.[134]

De algemene verplichting tot geheimhouding van bronnen en gegevens door de AIVD is beperkt tot daarvoor *in aanmerking komende* bronnen en gegevens. De verplichte bronbescherming strekt zich dus niet verder uit dan strikt noodzakelijk.[135] Als voorbeeld hiervan wordt genoemd het gebruik van open bronnen en gegevens: vermelding hiervan behoeft volgens de MvT niet op bezwaren te stuiten. In het algemeen is het zo dat zolang de lange termijn doeleinden van een dienst zich daartegen verzetten, de aan het doeleinde gerelateerde gegevens geheim dienen te zijn en blijven.[136] Dit geldt 'in het algemeen', dus niet altijd. Dit lijkt te betekenen dat er ruimte danwel mogelijkheden bestaan om van de beschermingsplicht af te wijken. Het is dan echter wel een uitzonderingssituatie.

De geheimhouding van gegevens van de AIVD is ook in ander opzicht niet altijd absoluut: in bepaalde gevallen zal de dienst tot verstrekking van gegevens over dienen te gaan. De AIVD is immers geen dienst met executieve bevoegdheden, dus zodra hij een dreiging constateert, zal hij de zogenoemde 'belangendragers' daarover inlichten zodat dezen over kunnen gaan tot het nemen van maatregelen die de dreiging wegnemen kunnen.

(B) Modaliteit van verstrekking: ambtsberichten

Verstrekkingen aan externe partijen vinden plaats door middel van de ambtsberichtprocedure, welke in het algemeen zijn basis heeft in artikel 36 WIV 2002. In 2004 en 2005 heeft de dienst enkele honderden ambtsberichten uitgebracht, waarvan de meeste aan de Immigratie- en Naturalisatiedienst (IND) en het OM. De politie ontvangt relevante ambtsberichten gewoonlijk via het OM.[137] Wanneer aan het OM wordt verstrekt, geldt echter niet de procedure van artikel 36 WIV 2002, maar die van artikel 38 WIV 2002.

Ook verstrekkingen aan justitie en politie op basis van artikel 38 gaan normaliter middels een ambtsbericht. Voordat een verstrekking plaatsvindt, wordt de landelijk officier van justitie inzake terrorismebestrijding geïnformeerd. Deze kan bepalen of de betreffende informatie ook daadwerkelijk gebruikt kan en mag worden

[133] *Kamerstukken II*, 1999/2000, 25 877, nr. 8, p. 42.
[134] *Kamerstukken II*, 1999/2000, 25 877, nr. 8, p. 42.
[135] *Kamerstukken* II, 1997/98, 25 877, nr. 3, p. 21.
[136] *Kamerstukken II*, 1999/2000, 25 877, nr. 8, p. 63-64.
[137] CTIVD (2006), p. 9.

(Van der Bel et al. 2009: 301-302). De landelijk officier van justitie krijgt van de AIVD inzage in alle relevante gegevens die voor de beoordeling van de juistheid van de in het ambtsbericht opgenomen gegevens nodig zijn.[138] De AIVD kan overigens ook op verzoek van een officier van justitie, advocaat-generaal of parkethoofd strafrechtelijk relevante informatie verstrekken.[139] Alhoewel de WIV 2002 formeel juridisch geen basis biedt voor het doen van een rechtmatigheidtoets, wordt deze toets in de praktijk ook door de landelijke officier van justitie gedaan.

Het uitbrengen van een ambtsbericht omtrent strafbare feiten of anderszins strafrechtelijk relevante gegevens is een discretionaire bevoegdheid. De AIVD kan hiertoe niet worden verplicht.[140] In bepaalde gevallen kan het verstrekken van strafrechtelijk relevante informatie immers leiden tot opsporingsactiviteiten van politie en justitie die schadelijk kunnen zijn voor de eigen operaties van de dienst. Bij de beoordeling of bepaalde informatie aan het OM ter beschikking moet worden gesteld, zal de dienst rekening houden met de concreetheid van de informatie, het belang van de nationale veiligheid en in bepaalde gevallen ook de veiligheid van de menselijke bron van de informatie (Van der Bel, et al. 2009: 302). De discretionaire ruimte van de dienst kent volgens de wetgever echter wel grenzen: "*het spreekt voor zich dat als er sprake is van ernstige misdrijven, de ruimte om te beslissen daar vervolgens geen mededeling over te doen uitermate klein – zo niet nihil- wordt.*"[141]

De wijze van verstrekken door de dienst hangt af van de te verwachten maatregelen die de ontvanger van de AIVD-informatie (mede) op basis van deze informatie zal nemen. De stelregel is dat als dergelijke te verwachten maatregelen de persoon op wie de informatie betrekking heeft in zijn rechtmatige belangen schaadt, de verstrekkingen door de AIVD middels een schriftelijk, open ambtsbericht worden gedaan (zie artikel 40 WIV 2002).[142] Met de term 'open' wordt bedoeld dat het ambtsbericht zo is opgesteld dat de betrokken persoon op wie het ambtsbericht betrekking heeft zonder bezwaar kennis kan nemen van het ambtsbericht.[143] Dit komt erop neer dat een ambtsbericht vrij summier is: het bevat vaak de naam van personen en een globale kwalificatie van de dreiging die volgens de dienst van de betreffende personen uitgaat.

(C) Parallelonderzoeken

Indien de AIVD informatie verstrekt aan het OM, dan bestaat het gevaar dat er parallelonderzoeken worden gedraaid. Geen rechtsregel verzet zich ertegen dat zowel de AIVD als het OM of de politie zelfstandig en daardoor mogelijk parallel onderzoek doet naar personen of groeperingen. Als beide diensten volgens de eigen taakstelling voldoende grond hebben om een onderzoek naar personen of groeperingen te verrichten, dan kan dat. Het gevaar van dergelijk parallel onderzoek schuilt in de mogelijkheid dat de ruimere mogelijkheden van de WIV 2002 worden toegepast en zo de strafvorderlijke waarborgen worden omzeild. De opsporingsinstantie mag echter niet de eigen strafvorderlijke bevoegdheden doelbewust niet toepassen zodat de

[138] Dit is een recht op basis van art. 38 lid 3, maar wordt in de praktijk als een plicht opgevat (Van der Bel et al. 2009: 302).
[139] *Ibid.*
[140] *Kamerstukken II*, 1997/98, 25877, nr. 3, p. 58. Zie ook Van der Bel et al. (2009: 302).
[141] *Kamerstukken II*, 1997/98, 25 877, nr. 3, p. 58.
[142] *Kamerstukken II*, 1997/98, 25 877, nr. 3, p. 55. De WIV 2002 noemt zelf de term 'ambtsbericht' niet, maar vereist slechts een schriftelijke verstrekking. In de praktijk komt dit echter neer op het verstrekken van een ambtsbericht.
[143] *Kamerstukken II*, 1997/98, 25 877, nr. 3, p. 55.

AIVD diens ruimere bevoegdheden kan gebruiken. Ook is het de opsporingsinstantie niet toegestaan om aan de AIVD te vragen of hij bepaalde bevoegdheden toepast waar de politie zelf niet over beschikt. De discretionaire bevoegdheden van de AIVD met betrekking tot het verstrekken van informatie aan het OM maakt het wel mogelijk om op verzoek van het OM informatie te verstrekken. Geen rechtsregel belet het OM of de opsporingsdiensten om dergelijke informatie te vragen.[144]

3.5 AIVD-informatie in het strafproces

Over AIVD-informatie in het strafproces zijn wij zeer summier. De fase van het onderzoek ter terechtzitting valt immers buiten de scope van ons onderzoek.[145] In deze sectie behandelen wij allereerst (A) het gebruik van AIVD-informatie als start- en sturingsinformatie en vervolgens (B) het gebruik van AIVD-informatie als bewijs in strafzaken.

(A) Start- en sturingsinformatie

Informatie afkomstig van de AIVD kan een verdenking opleveren op grond waarvan bijzondere opsporingsbevoegdheden kunnen worden toegepast. Ook voor informatie afkomstig van de AIVD geldt dat zij in voldoende mate concrete feiten of omstandigheden moet opleveren waaruit het redelijke vermoeden voortvloeit. Het probleem van AIVD-informatie is echter de beperkte toetsingsmogelijkheid. De rechtmatigheid van de verkrijging van de AIVD-informatie waar de verdenking uit voortvloeit, kan niet worden getoetst, maar dit doet niets af aan het feit dat deze informatie een verdenking kan opleveren.[146] Indien de juistheid van de AIVD-informatie wordt onderzocht en dit onderzoek geen aanvullende belasting oplevert, kan de informatie echter onvoldoende zijn om een redelijke verdenking op te baseren (Van der Bel et al. 2009: 305).[147] Daarnaast kan de informatie altijd aanleiding zijn om lopende opsporingsonderzoeken bij te sturen. Met andere woorden: AIVD-informatie kan gebruikt worden als start- en sturingsinformatie.

(B) Bewijs

In principe is een ambtsbericht een schriftelijk bescheid als bedoeld in artikel 344 lid 1 onder 3 WvSv en kan het dienen als bewijs in een strafzaak (Van der Bel et al. 2009: 314). Het probleem van het gebruiken van AIVD-ambtsberichten als bewijs ligt in de beperkte toetsbaarheid van met name de betrouwbaarheid van de in het ambtsbericht vervatte gegevens. De AIVD heeft immers zoals hierboven al is gesteld een plicht om zijn bronnen en *modus operandi* geheim te houden. Dit maakt dat AIVD-ers in de regel ten overstaan van de strafrechter geen inzicht kunnen geven in

[144] Hof Den Haag 2 oktober 2008, LJN BF3987 (Zaak Piranha). Zie ook HR 5 september 2006, LJN AV 4149 (Zaak Eik); HR 13 november 2006, LJN BA 2553 (Zaak BPRC). Behandeld in Van der Bel et al. (2009: 306-307). Zie ook Van der Woude (2010: 212 e.v.).

[145] Wij verwijzen voor een uitgebreide behandeling van het gebruik van AIVD-informatie in het strafproces naar: Vervaele 2005; Van der Bel et al. 2009; Hirsch Ballin 2012.

[146] Zie: Rechtbank Rotterdam, 5 juni 2003, LJN AF 9546. Zie ook: HR 5 september 2006, LJN AV 4149 (Zaak Eik).

[147] Zij verwijzen naar Hoge Raad 11 maart 2008, LJN BB7662 (Hoog Catharijne Zaak). In die zaak werd aan de AIVD anoniem telefonisch informatie verstrekt wat vervolgens aan de districtsrecherche is doorgegeven. Onderzoek door verschillende rechercheteams heeft geen aanvullende informatie opgeleverd, hetgeen de informatie ontoereikend maakte voor een verdenking.

de achterliggende informatie op grond waarvan het ambtsbericht tot stand is gekomen (Van der Bel et al. 2009: 307-308). Een betrouwbaarheidstoets is voor de overtuigingskracht van het bewijs echter essentieel, en gezien de beperkte mogelijkheden met betrekking tot AIVD-informatie zal de rechter per casus moeten beoordelen of het materiaal voor het bewijs gebruikt mag worden.[148]

Met de Wet afgeschermde getuigen[149] heeft de wetgever geprobeerd om voor de beperkte toetsbaarheid van AIVD-informatie een oplossing te vinden. De rechter-commissaris kreeg in deze wet meer ruimte om bij het verhoor van getuigen rekening te houden met de staatsveiligheid. De wet voorziet in twee afschermingsmogelijkheden van informatie waarbij de staatsveiligheid mogelijk in het geding is. Allereerst kan de openbaarmaking van bepaalde gegevens worden belet indien er gegrond vermoeden bestaat dat door de openbaarmaking van die gegevens de staatsveiligheid wordt geschaad. De rechter-commissaris kan onderzoek doen naar hoe bepaalde AIVD-informatie is verkregen en hiertoe getuigen horen. Hij kan dan op dusdanige wijze verslag leggen dat bepaalde gegevens niet worden vastgelegd.[150] Ten tweede kan de rechter-commissaris medewerkers van de AIVD afgeschermd verhoren, indien redelijkerwijs kan worden aangenomen dat het belang van de staatsveiligheid dat vereist. De afscherming houdt in dat de identiteit van de getuige geheim blijft en het verhoor buiten de aanwezigheid van de officier van justitie en de verdediging plaatsvindt. De verdediging en de officier van justitie krijgen wel de gelegenheid om schriftelijk danwel door middel van telecommunicatie via de rechter-commissaris vragen te stellen aan de getuige (Van der Bel et al. 2009: 313).

3.6 De RID

Een bijzonder organisatieonderdeel van de AIVD is de Regionale Inlichtingendienst (RID). Deze dienst is ondergebracht bij de regionale politiekorpsen en het KLPD maar verricht voor een belangrijk deel werkzaamheden voor de AIVD. Naast werkzaamheden voor de AIVD heeft de RID ook een openbare orde taak. Het verzamelen van inlichtingen op het gebied van de openbare orde doet de RID onder het gezag van de burgemeester. Deze 'dubbele pet' van de RID-er is van belang voor de verhouding tussen de AIVD en de politie: het ene moment is een RID-er politieman, het andere moment is hij AIVD-er. Zodoende staat de RID in een bijzondere relatie tot de politie en de AIVD. In deze sectie bespreken we achtereenvolgens de AIVD-taak van de RID (subsectie 3.6.1), de relatie van de RID met de opsporing (subsectie 3.6.2) en tot slot de openbare orde taak van de RID (subsectie 3.6.3).

3.6.1 De AIVD-taak van de RID

Wanneer de RID werkzaamheden voor de AIVD verricht, dan doet hij dit op basis van de WIV 2002 en in ondergeschiktheid aan de AIVD. De RID fungeert als de 'ogen en oren' van de AIVD (Hoogenboom 2009: 17). De dienstleiding van de AIVD stelt samen met de korpsleiding van elk regiokorps jaarlijks een zogenoemd 'inlichtingen-behoefteplan' vast. Dit plan functioneert als een samenwerkingsconvenant tussen de AIVD en de afzonderlijke regiokorpsen. Het bevat de prioriteiten voor dat jaar, alsmede de verwachte prestaties en resultaten. Het

[148] HR 5 september 2006, LJN AV4122 (Zaak Eik).
[149] Wet van 28 september 2006, stb. 2006, 460.
[150] Het betreft hier een wijziging van artikel 187d WvSv. Zie: Van der Bel et al. (2009: 312).

benoemt concreet de uren die de RID aan AIVD-taken dient te besteden (Commissie Havermans 2004: 98). Daarnaast benoemt het gezamenlijke operationele activiteiten, zoals de inzet van agenten. De korpschef bepaalt hoeveel procent van de werkzaamheden gericht is op openbare orde werk en hoeveel op inlichtingenwerk. Aan het plan is een databank gekoppeld waarin de actuele AIVD-onderzoeken en verzoeken om informatie per team zijn opgenomen. Door middel van het raadplegen van de database kan de RID inzicht verkrijgen in de specifieke behoeften van de AIVD (CTIVD 2007: 4). Voor 2004 werd er een heel andere procedure gehanteerd. Toen werden er operationele activiteitenplannen opgesteld door de AIVD. Deze plannen vloeiden voort uit de informatievragen van afzonderlijke teams. De RID-en ontvingen een lijst met vragen en informatieverzoeken, maar deze lijst was vaak zeer omvangrijk omdat alle teams van de AIVD afzonderlijk vragen aan het plan toe konden voegen. Daarnaast was er dikwijls sprake van overlap tussen de vragen van de teams. Om het proces te stroomlijnen en de afstemming tussen RID en AIVD te verbeteren, is de bovenstaande procedure van het inlichtingen behoefteplan ontwikkeld.

Op het moment dat de RID-er inlichtingenwerk verricht, is hij feitelijk een AIVD-er (een 'artikel 60 ambtenaar', vernoemd naar het artikel uit de WIV waarin de status wordt geregeld van bepaalde functionarissen die werkzaamheden voor de AIVD verrichten maar daar niet formeel in dienst zijn). De RID kan doordringen in de haarvaten van de samenleving, wat voor de AIVD zelf vaak gezien de beperkte capaciteit niet mogelijk is (Commissie Havermans 2004: 96). De AIVD, kan met de mensen en middelen die hij tot zijn beschikking heeft onmogelijk heel Nederland in de gaten houden en valt voor ondersteuning terug op de RID. De RID-er die werkzaamheden namens de AIVD verricht, heeft daarom in principe de beschikking over het gehele arsenaal van bevoegdheden uit de WIV 2002. In de praktijk blijkt echter dat de RID met name wordt ingezet bij het runnen van agenten. Vanwege de bijzondere informatiepositie op lokaal gebied, is de RID bij uitstek de aangewezen instantie om agenten te begeleiden die in bepaalde lokale groeperingen zijn geïnfiltreerd. In de praktijk komt het dan ook vaak voor dat agenten worden gerund door een runner van de RID en een acquisiteur/operateur van de AIVD tezamen (Van der Bel et al. 2009: 281). De reden waarom de inzet van bijzondere inlichtingenmiddelen door een RID wordt beperkt tot het runnen van agenten is gelegen in het feit dat de AIVD vaak van mening is dat de noodzakelijke expertise bij de RID ontbreekt om bijvoorbeeld observaties uit te voeren (CTIVD 2008: 10).

De RID heeft naast het bijlopen van AIVD-onderzoeken met betrekking tot agenten ook nog andere operationele taken. Zo kan de RID worden ingeschakeld door (andere) politieambtenaren op het moment dat zij over informatie beschikken die mogelijk interessant is voor de AIVD. Daarnaast kan de uitvoering van de openbare orde taak informatie genereren die mogelijk voor de AIVD interessant is. De RID kan ook, op uitdrukkelijk verzoek van de AIVD, in politiebestanden zoeken naar mutaties met betrekking tot AIVD-subjecten.

Een belangrijke beperking van de activiteiten van de RID wordt door de commissie van toezicht beschreven: de RID kan niet zelfstandig op basis van artikel 60 WIV 2002 onderzoekshandelingen verrichten ten behoeve van de AIVD-taak, ook niet indien het zaken betreft die ooit bij de RID onder de aandacht zijn gebracht door de AIVD. Er moet dus altijd een opdracht van de AIVD zijn. Voor een goede samenwerking en een optimale inzet van de RID is het van belang dat de AIVD actief sturing geeft aan de RID en deze voorziet van de noodzakelijke informatie. Volgens de commissie is het van belang dat de RID een volledig overzicht heeft van alle

AIVD-onderzoeken die in de regio draaien. Op die manier kan de RID daadwerkelijk invulling geven aan de oog- en oorfunctie. Ook is het binnen de WIV 2002 de RID niet toegestaan om op eigen initiatief de onderlinge samenwerking te zoeken. RID-en mogen pas onderling samenwerken indien dit in uitdrukkelijke opdracht van de AIVD geschiedt. Vanzelfsprekend houdt de AIVD bij deze samenwerking de controle en regie (Van der Bel et al. 2009: 282).

3.6.2 De RID en de opsporing

Net als de AIVD heeft de RID op basis van artikel 9 WIV 2002 bij het uitvoeren van de AIVD-taak geen bevoegdheid tot het opsporen van strafbare feiten. Volgens de Commissie Havermans staat de RID volledig buiten de opsporing (2004: 282). Tussen de CIE en de RID is een wereld van verschil, zowel in taakstelling, aandachtsgebied als organisatiecultuur (Hoogenboom 2009: 20). Indien de RID gegevens heeft verzameld in het kader van zijn AIVD-taak, dan kan deze informatie niet rechtstreeks aan de recherche worden verstrekt: de algemeen geldende procedure van het ambtsbericht is de aangewezen weg voor een dergelijke verstrekking. Een direct contact tussen de RID en de recherche met als doel het verstrekken van AIVD-informatie is dus niet mogelijk: het is de AIVD die dergelijke informatie kan verstrekken. De RID-er verliest echter niet zijn bevoegdheid tot het verrichten van opsporingshandelingen, en het is dan ook (formeel-juridisch) niet ondenkbaar dat een RID-er tot het verrichten van opsporingshandelingen overgaat op het moment dat hij een strafbaar feit constateert (Van der Bel 2009: 282). De gehanteerde opsporingsbevoegdheden mogen echter niet worden toegepast ten behoeve van de inlichtingentaak en andersom. Alhoewel er formeel juridisch geen belemmeringen lijken te zijn voor opsporing door een RID, zal het in de praktijk niet wenselijk zijn om de RID te laten opsporen. Het is voor de RID al lastig om de AIVD-taak te scheiden van de openbare orde taak (zie de volgende subsectie), laat staan dat hier ook nog een opsporingsdimensie aan wordt toegevoegd.

3.6.3 De openbare orde taak van de RID

Naast de bovengenoemde inlichtingentaak heeft de RID zoals gezegd ook een openbare orde taak welke hij uitoefent onder gezag van de burgemeester. De RID dient de bewegingen van bepaalde groepen in kaart te brengen en de burgemeester te adviseren omtrent te nemen beslissingen in het publieke domein. De RID adviseert bijvoorbeeld over voetbalvandalisme en hardnekkige problemen met jongerengroepen (Commissie Havermans 2004: 96). Een belangrijke regel is dat de RID zich bij de openbare orde taak niet mag richten op individuen, maar slechts op de bewegingen en activiteiten van groepen van personen. Informatie over individuen wordt in het kader van de openbare orde taak dan ook slechts verzameld indien deze inzicht geeft in de bewegingen en activiteiten van een groep van personen. In de praktijk zal dit echter weinig problematisch zijn: iemand behoort immers al snel tot een groep. Alhoewel het gaat om met welk doel gegevens worden verzameld (het verkrijgen van inzicht in een groep of het verkrijgen van inzicht in een individu), biedt dit ‘groepscriterium’ in de praktijk de burger weinig bescherming. Als de RID echt gegevens over een persoon wil verzamelen in het kader van de openbare orde taak, dan zal hij vrij gemakkelijk kunnen aantonen dat de informatie nodig is voor inzicht in een groep en daarmee is de verzameling al snel gerechtvaardigd.

De basis voor de openbare orde taak van de RID is artikel 2 jo. 13 Politiewet 1993, artikel 172 Gemeentewet en de Handleiding informatie-inwinning openbare orde. Uit rechtspraak met betrekking tot artikel 2 en 13 Politiewet 1993 volgt dat de RID niet een meer dan een beperkte inbreuk op de persoonlijke levenssfeer mag maken.[151] Van de WIV-bevoegdheden mag de RID bij het uitvoeren van de openbare orde taak geen gebruik maken. De RID kan op basis van artikel 2 Politiewet 1993 wel informanten runnen en niet stelselmatige observatie toepassen. In de praktijk blijken de RID-en echter wel degelijk gebruik te maken van bevoegdheden die een meer dan beperkte inbreuk maken op de persoonlijke levenssfeer, en blijft de gegevensverzameling niet beperkt tot groepen van personen maar betreft het ook vaak individuen. De openbare orde taak heeft de laatste jaren namelijk een belangrijke ontwikkeling doorgemaakt. In het kader van de openbare orde taak verrichten de RID-en vandaag de dag veel onderzoek naar radicalisering van individuen, een onderwerp dat nauw verbonden is met terrorismebestrijding. Hierbij worden bevoegdheden als het runnen van agenten en stelselmatige observatie toegepast. De wettelijke grondslag voor de inzet van deze bevoegdheden in het kader van de openbare orde taak lijkt echter te ontbreken (CTIVD 2007: 15). Dit komt waarschijnlijk omdat de openbare orde taak en de AIVD taak met name bij onderzoeken naar radicalisering in de praktijk dikwijls door elkaar heen lopen.

De huidige regelgeving stelt geen grenzen aan de openbare orde taak van de RID en voorkomt dan ook niet dat de RID zich bij het uitvoeren van die taak begeeft op AIVD-terrein (CTIVD 2007: 13; Hoogenboom 2009: 79). Het gevaar bestaat dat de RID onderzoeken naar radicalisering te gemakkelijk onder de noemer van de AIVD-taak schuift om gebruik te kunnen maken van de verregaande bevoegdheden uit de WIV 2002. Dit lijkt in de praktijk echter geen groot gevaar: weliswaar beschikt de RID *de jure* over meer ingrijpende bevoegdheden wanneer zij werkzaamheden verricht in het kader van de AIVD-taak, *de facto* lijkt de toepassing van de bijzondere inlichtingenmiddelen te worden beperkt tot het runnen van agenten (Van der Bel et al. 2009: 285). De hierboven beschreven praktijk geeft overigens al aan dat de RID zich, al dan niet gedwongen door operationele noodzaak en onduidelijke regelgeving, weinig aan de kaders van de regelgeving gelegen laat liggen. Bij de openbare orde taak worden immers nu ook al bevoegdheden als het runnen van agenten en stelselmatige observatie ingezet. De toepassing van deze bevoegdheden maakt een meer dan beperkte inbreuk op de persoonlijke levenssfeer van de burger, hetgeen een specifieke wettelijke grondslag vereist. Deze ontbreekt vandaag de dag, waarmee het optreden van de RID voor zover deze bevoegdheden worden toegepast als onrechtmatig kan worden gekenschetst.[152] Het is in dit opzicht overigens goed om te realiseren dat de figuur van de agent een wezenlijk andere is dan die van de informant: de eerste wordt door de AIVD gestuurd. In het kader van de openbare orde taak van de RID past deze de bevoegdheid zelfstandig toe, zonder regie van de AIVD. Zoals in hoofdstuk vier nog wordt behandeld, is een speciale variant van de figuur van

[151] Zie het Zwolsmanarrest, HR 19 december 1995, NJ 1996, 249.

[152] Volgens Van der Bel et al. (2009) vervalt hiermee het voordeel voor de RID om een onderzoek onder de AIVD-taak te scharen. Ze passen die bevoegdheden immers toch al toe. Het voordeel is volgens hen dat de burgemeester de RID direct kan aansturen en de informatie die de RID op deze manier verzamelt, kan direct aan hem worden verstrekt. Indien het onder de AIVD-taak valt, is het aan de AIVD om, binnen het regime van de WIV 2002, de gegevens te verstrekken (zie Van der Bel et al. 2009: 285-286). Dit is een enigszins verwonderlijk standpunt. De toepassing van de bevoegdheden is immers wederrechtelijk, het is een praktijkvoordeel waarvan eigenlijk helemaal geen sprake mag zijn. Daarnaast zal het voordeel voor de burgemeester teniet worden gedaan door het enkele feit dat onder zijn gezag en daarmee zijn verantwoordelijkheid wederrechtelijk is opgetreden.

de agent in de opsporing (de 'criminele burgerinfiltrant') over het algemeen uit den boze, en dat terwijl het Wetboek van Strafvordering daarvoor wel een juridische basis biedt (126w en 126x WvSv).[153] De criminele burgerinfiltrant (en de toen nog ontbrekende juridische grondslag) was zelfs één van de directe aanleidingen voor de IRT-affaire. Het is daarom verontrustend dat de RID, een ander onderdeel van de politie, inmiddels wel gebruik maakt van een vergelijkbaar figuur. Het is voorts niet ondenkbaar dat de vruchten van dit inlichtingenmiddel, de informatie die de agent verstrekt, uiteindelijk via een proces-verbaal aan de recherche wordt verstrekt. Dit zou een bijzondere onwenselijke vermenging van het politieke en criminele inlichtingenwerk betekenen. De omvang van deze mogelijk onrechtmatige manier van werken is ons tijdens het veldwerk niet duidelijk geworden. Kortom, op dergelijke operationele informatie hebben wij geen zicht gehad.

3.7 De politiek-bestuurlijke context van de AIVD

De AIVD verricht zijn werkzaamheden niet in een vacuüm: de dienst wordt aangestuurd en zijn werkzaamheden worden gecontroleerd en getoetst aan geldende wet- en regelgeving. In deze sectie zullen wij deze politiek-bestuurlijke context van de AIVD kort behandelen. We beginnen bij de sturing van de AIVD (subsectie 3.7.1). Vervolgens behandelen we de belangrijkste wijze waarop toezicht wordt gehouden op de taakuitvoering en werkzaamheden van de AIVD. Dit toezicht wordt door de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) uitgevoerd (subsectie 3.7.2).

3.7.1 Sturing

De dagelijkse sturing van de AIVD ligt met name bij het hoofd van de dienst (en diens plaatsvervanger). In de praktijk is hij door de Minister van Binnenlandse Zaken en Koninkrijksrelaties gemandateerd voor bijvoorbeeld de toepassing van bijzondere inlichtingenmiddelen (artikel 19 lid 1 WIV 2002). Het hoofd kan deze bevoegdheid op zijn beurt weer doormandateren. Bij de toepassing van bepaalde, zeer diepingrijpende bevoegdheden zoals het met een technisch hulpmiddel gericht afluisteren van gesprekken (artikel 25 lid 2 WIV 2002) is mandatering overigens niet mogelijk (Van der Bel 2009: 260).

De beheersmatige en inhoudelijke verantwoordelijkheid voor de AIVD ligt bij de Minister van Binnenlandse Zaken en Koninkrijksrelaties. De minister is in dit kader degene die bepaalde diepingrijpende bijzondere inlichtingenmiddelen kan laten toepassen danwel mandateren aan het hoofd van de AIVD. Met betrekking tot de D-taak (buitenlandtaak) van AIVD is het met name de minister-president die de sturing heeft. Hij wijst in overeenstemming met de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Defensie en in overeenstemming met de Minister van Buitenlandse Zaken de landen en onderwerpen aan waarop de AIVD zich in het kader van deze D-taak richt. Op het gebied van de terrorismebestrijding heeft de Minister van Veiligheid en Justitie een coördinerende taak, maar hij beschikt niet over sturingsmogelijkheden ten opzichte van de AIVD.

[153] Op de inzet van de criminele burgerinfiltrant rust echter een parlementair moratorium. Zie: *Kamerstukken II* 1998/99, 25 403 en 23 251, nr. 33. Hierop kan echter een uitzondering worden gemaakt bij opsporingsonderzoeken naar terroristische misdrijven: zie *Kamerstukken II*, 2002/03, 27 834, nr. 28.

Op beleidsmatig niveau worden de onderwerpen met betrekking tot de AIVD besproken in twee onderraden van de ministerraad, te weten de Raad voor de Nationale Veiligheid en de Raad voor de Veiligheid en Rechtsorde. De Raad voor de Nationale Veiligheid is in 2004 ingesteld met als doel tot een betere coördinatie van terrorismebestrijding te komen. In deze raad hebben de minister-president, de vice-premiers, de Ministers van Binnenlandse Zaken en Koninkrijksrelaties, Buitenlandse Zaken, Veiligheid en Justitie en Integratie- en Vreemdelingenzaken zitting. Het mag duidelijk zijn dat vanwege de bezetting van de raad de coördinatie op het gebied van terrorismebestrijding goed uit de verf kan komen. Operationele aangelegenheden worden hier echter nauwelijks besproken: het gaat met name om beleidsmatige en organisatorische aangelegenheden (Commissie Havermans 2004: 83-84). De Raad voor de Nationale Veiligheid heeft ook een soort 'ambtelijk voorportaal', het Comité Verenigde Inlichtingendiensten Nederland (CVIN). Dit comité coördineert werkzaamheden en bevordert de samenwerking tussen inlichtingen- en veiligheidsdiensten. Het bestaat uit de DG's van de betrokken departementen en de hoofden van de AIVD en de MIVD. De behandelde onderwerpen zijn gelijk aan de onderwerpen die in de Commissie Nationale Veiligheid worden behandeld. Een vast agendapunt is een evaluatie van de dreiging tegen de nationale veiligheid.

Op zichzelf is het bovenstaande vrij duidelijk: de Minister van Binnenlandse Zaken heeft in het algemeen het gezag en de verantwoordelijkheid over de AIVD, zeker daar waar het de A-taak betreft. De coördinatie tussen verschillende diensten vindt plaats in de commissie Nationale Veiligheid en het Comité Verenigde Inlichtingendiensten. De coördinatie van de diensten is echter kennelijk zo'n belangrijk punt, dat er naast bovengenoemde organisatorische eenheden ook nog eens drie nationaal coördinatoren in het leven zijn geroepen die allen het inlichtingenwerk dienen te coördineren: de coördinator voor de Inlichtingen- en Veiligheidsdiensten (IVD), de Nationaal Coördinator Bewaken en Beveiligen (CBB) en de Nationaal Coördinator Terrorismebestrijding (NCTb). We laten de coördinator CBB verder buiten beschouwing omdat zijn rol in de verhouding tussen opsporing- en inlichtingendiensten beperkt is. Deze figuur is inmiddels onderdeel geworden van de NCTb. Sinds 1 juli 2011 vallen de terreinen nationale veiligheid en terrorismebestrijding onder één coördinator: de Nationale Coördinator Terrorismebestrijding en Veiligheid (NCTV). Hieronder staan wij kort stil bij de NCTV, waarbij we ons beperken tot het onderdeel terrorismebestrijding.

De taak van de NCTV is het coördineren en bewaken van de samenwerking tussen de circa twintig instanties die zijn betrokken bij terrorismebestrijding. Uit hoofde van deze functie is het NCTV aangesteld als hoofd van het Gezamenlijk Comité Terrorismebestrijding. Dit comité richt zich op strategie en beleid. Voor de meer operationele samenwerking is het Coördinerend Overleg Terrorismebestrijding in het leven geroepen (Commissie Havermans 2004: 85). Leden van het comité zijn de diverse betrokken ministeries (Veiligheid en Justitie, Binnenlandse zaken en Koninkrijksrelaties, defensie en dergelijke) en het College PG's, de AIVD, de MIVD, het KLPD en de Kmar. De NCTV valt onder de verantwoordelijkheid van zowel de Minister van Veiligheid en Justitie als de Minister van Binnenlandse Zaken en Koninkrijksrelaties. Organisatorisch en beheersmatig is de NCTV ondergebracht bij het Ministerie van Veiligheid en Justitie. De NCTV heeft een aantal directies, waaronder een directie Kennis en Analyse. Dit is een landelijk informatieknooppunt waar informatie afkomstig van verschillende bronnen (bestuurlijke en wetenschappelijke instanties en inlichtingen- en veiligheidsdiensten zoals de AIVD en onderdelen van de politie) wordt samengebracht en gecombineerd wordt

geanalyseerd. De directie produceert op basis van deze informatie een totaalbeeld van terrorisme en terrorismebestrijding, verricht trend- en fenomeenanalyses en geeft beleidsmatig advies. Een driemaandelijks Dreigingsbeeld Terrorisme is één van de producten van de directie. Wat de precieze verhouding is tussen de CT-infobox en de directie Kennis en Analyse van de NCTV is niet helemaal duidelijk (Commissie Havermans 2004: 87).

3.7.2 De Commissie van toezicht op de Inlichtingen- en Veiligheidsdiensten

Eén van de problematische aspecten van inlichtingen- en veiligheidsdiensten is de mogelijke gebrekkige controle van deze diensten vanwege de verregaande geheimhouding. In die gevallen waarin AIVD-informatie in een strafprocedure wordt ingebracht (als start- en sturingsinformatie of als bewijs), zal de strafrechter voor zover mogelijk een zekere mate van controle willen uitoefenen over de betrouwbaarheid en rechtmatigheid van de informatie. De controle en het toezicht op de werkzaamheden van de AIVD ligt echter niet primair bij de rechterlijke macht. Het optreden van de AIVD heeft zelden rechtsgevolgen voor een burger en de dienst zal daarom niet snel in een rechtszaal verschijnen. Toch kent Nederland zoals eerder gezegd bepaalde maatregelen die voor een zekere mate van transparantie van de inlichtingendiensten moeten zorgen. De belangrijkste van deze maatregelen is de instelling van een Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD).[154]

De CTIVD bestaat uit drie leden welke op voordracht van de Tweede Kamer worden benoemd. Haar belangrijkste taak is het houden van toezicht op de rechtmatigheid van het handelen van de AIVD en de MIVD en het informeren van de betrokken ministers over haar bevindingen.[155] Hiertoe verricht de commissie zogenoemde 'diepteonderzoeken'. Een diepteonderzoek is gericht op een compleet onderzoeksdossier van de AIVD of de MIVD over een vooraf vastgestelde periode, waarbij de door de diensten verrichte handelingen en uitgeoefende bijzondere bevoegdheden worden beoordeeld aan de hand van criteria, zoals rechtmatigheid, noodzakelijkheid, proportionaliteit, en subsidiariteit. Het diepteonderzoek kan zich overigens ook op lopende onderzoeken richten.[156] Van de diepteonderzoeken wordt verslag gedaan in openbare toezichtrapporten, welke te zien zijn op de website van de commissie.[157] Ten aanzien van bepaalde onderwerpen voert de commissie ook een monitoring uit. Deze monitoring geschiedt steekproefsgewijs.

Naast de diepteonderzoeken kan de commissie de minister ook gevraagd en ongevraagd adviseren over de afhandeling van klachten over de AIVD en de MIVD. De advisering beperkt zich niet tot de rechtmatigheid van het optreden van de AIVD: ook over de doelmatigheid kan worden geadviseerd, zo meent althans de commissie.[158] In de Memorie van Toelichting op de WIV 2002 valt echter te lezen dat het toezicht achteraf op de rechtmatige uitvoering van de bepalingen van die wet ziet, een doelmatigheidstoets wordt hier expliciet uitgesloten.[159] De commissie is kennelijk

[154] Zie voor een uitgebreide en kritische behandeling van de CTIVD: Fijnaut (2012). Zie ook: CTIVD (2012).
[155] Artikel 64 lid 2 WIV 2002. Omdat de commissie geen bestuursorgaan in de zin van de Algemene Wet Bestuursrecht is, is het niet mogelijk om tegen haar oordelen en daarmee samenhangende besluiten bezwaar te maken of in beroep te gaan.
[156] Zie: www.ctivd.nl, gezien op 7 december 2009. Zie ook Van der Bel et al. (2009: 262).
[157] http://www.ctivd.nl/, gezien op 7 december 2009.
[158] *Ibid*.
[159] MvT *Kamerstukken II*, 1997/98. 25 877, nr. 3, p. 79 en 81.

van mening dat zij, indien zij op doelmatigheidsproblemen stuit, een taak heeft om hier melding van te maken. Wellicht heeft zij hierin gelijk: het zou vreemd zijn als de commissie misstanden constateert maar deze niet door mag geven. Dat het onderzoek van de commissie in de praktijk ook aan doelmatigheidsvraagstukken zal raken, is dan ook een wenselijke situatie. Het is echter niet wenselijk (of toegestaan) dat de commissie zelfstandig onderzoeken opstart met als doel het onderzoeken van de doelmatigheid van de dienst.

De commissie kan zoals gezegd ook een steekproef doen: een kortlopend onderzoek naar de rechtmatigheid van (delen van) onderzoeken door de AIVD en MIVD door één van de leden van de commissie. Naar aanleiding van de bevindingen van een steekproef kan vervolgens een diepteonderzoek worden ingesteld.

De commissie kan geen bindende besluiten nemen met betrekking tot de operationele werkzaamheden van de AIVD en de MIVD. Mocht zij tijdens het uitvoeren van haar taak op iets stuiten waarvan zij van mening is dat dit dient te stoppen, dan kan zij daarvan melding maken aan de minister. Het is aan de minister om vervolgens een besluit te nemen.[160]

Voor het uitvoeren van haar taak heeft de commissie allereerst rechtstreeks toegang tot alle in het kader van de WIV 2002 en de Wet op de veiligheidsonderzoeken verwerkte gegevens. De commissie mag kennis nemen van elk stuk dat door haar wordt aangetroffen en wat volgens haar relevant is voor een door haar ingesteld onderzoek, aldus artikel 73 lid 1 WIV 2002. Daarnaast is een ieder betrokken bij de uitvoering van de hierboven genoemde wetten verplicht om desgevraagd de noodzakelijke gegevens aan de commissie te verstrekken en voor het overige zijn medewerking te verlenen. De AIVD kan echter aangeven dat bepaalde informatie in het belang van de nationale veiligheid uitsluitend ter kennisneming van de commissie dient te blijven (artikel 73 WIV lid 2 2002).

De commissie beschikt voorts over een aantal andere bevoegdheden. Zo kan zij getuigen en deskundigen oproepen inlichtingen te verstrekken of voor haar te verschijnen.[161] Hiernaast heeft de commissie de bevoegdheid plaatsen, met uitzondering van een woning zonder toestemming van de bewoner, te betreden voor zover dat voor de vervulling van haar taak redelijkerwijs nodig is (artikel 77 WIV 2002).

Al met al kent het Nederlandse systeem een verregaande toezicht op de rechtmatigheid van het optreden van de AIVD, en tot op zekere hoogte ook op de doelmatigheid. De commissie van toezicht is zeker geen papieren tijger: zij beschikt over verregaande bevoegdheden voor het vervullen van haar taak en de dienst heeft hier in vrijwel alle opzichten aan mee te werken. Omdat deze commissie ook nog volledig onafhankelijk van de dienst functioneert, is het de belangrijkste waarborg voor de in een democratie gewenste en noodzakelijke transparantie. Het is echter niet het enige toezicht- en controle instrument van het Nederlandse systeem.

Naast de commissie bestaan er nog enkele andere toezicht- en controle-instrumenten, zoals de vertrouwelijke commissie voor de Inlichtingen- en Veiligheidsdiensten, waarin alle fracties van de Tweede Kamer zitting hebben. Het kabinet licht de Tweede Kamer in over diverse werkzaamheden van de inlichtingendiensten. Dit is een vertrouwelijke commissie en overleg vindt achter gesloten deuren plaats (Commissie Havermans 2004: 29). Omdat ze te ver van het

[160] Brief minister BZK, *Kamerstukken II*, 1999/2000, 25 877, nr. 59, p. 18.
[161] Weigerachtige getuigen kunnen zelfs een bevel tot medebrenging tegemoet zien. Zie artikel 74 lid 6 WIV 2002.

eigenlijke onderwerp van ons onderzoek staan, laten wij deze toezicht- en controle instrumenten verder buiten beschouwing.

3.8 Hoofdstukconclusie: antwoord OV 1

In dit hoofdstuk hebben wij de Nederlandse veiligheidsdienst behandeld. Deze laatste sectie plaatst de bevindingen uit dit hoofdstuk in het licht van de HP-kenmerken van de veiligheidsdiensten zoals beschreven in hoofdstuk twee. Deze kenmerken zijn (A) de bescherming van de nationale veiligheid, (B) het geven van voorwaarschuwingen en het proactief signaleren van bedreigingen, (C) de intelligence cyclus als werkproces en (D) verregaande geheimhouding. In deze laatste sectie van dit hoofdstuk werken wij het antwoord op OV 1 verder uit aan de hand van de AIVD. We herhalen hierbij OV1: *Wat zijn de traditionele kenmerken van veiligheidsdiensten en de politie?*

A: HP-kenmerk 1: nationale veiligheid

De AIVD is verantwoordelijk voor de bescherming van de nationale veiligheid. Hiermee voldoet de AIVD aan het eerste HP-kenmerk (gedeeltelijk antwoord OV1). Deze taak wordt verder (juridisch) uitgewerkt in artikel 6 lid 1 sub a WIV 2002, ook wel de A-taak genoemd. Onderwerpen die raken aan de nationale veiligheid behoren tot de taak van de AIVD, hetgeen een duidelijke aanwijzing is voor de formele verhouding tussen de AIVD en de politie. In dit hoofdstuk is dan ook de reikwijdte van het begrip 'nationale veiligheid' onderzocht, ervan uitgaande dat dit inzicht geeft in een deel van de formele verhouding. Dit blijkt echter niet het geval te zijn. 'Nationale veiligheid' is een open begrip dat door de AIVD zelfstandig kan worden ingevuld. Het is dus zeer casuïstisch, en de dienst zal per geval beoordelen of en in hoeverre er sprake is van een bedreiging van de nationale veiligheid. Met name islamitisch terrorisme is één van de aandachtsgebieden van de dienst in het kader van de A-taak. Daarnaast heeft de dienst zich in het verleden ook gericht op de bestrijding van georganiseerde criminaliteit, maar dat is vandaag de dag geen zelfstandig aandachtsgebied meer.

B: HP-kenmerk 2: voorwaarschuwingen en proactief signaleren van bedreigingen

Om vast te stellen of en in hoeverre er sprake is van een mogelijke bedreiging van de nationale veiligheid staan er verschillende bevoegdheden ter beschikking aan de dienst. Deze hebben allemaal één ding gemeen: primair gaat het om het verzamelen van informatie zodat de dienst tijdig een voorwaarschuwing kan geven. De kerntaak van de AIVD is het opbouwen en in stand houden van een informatiepositie teneinde de nationale veiligheid te beschermen. Dit kan alleen indien er tijdig zicht is op mogelijke bedreigingen: de dienst zal proactief inlichtingen moeten verzamelen omtrent bedreigingen en aan de hand daarvan een voorwaarschuwing moeten geven aan de belangenhebbenden (gedeeltelijk antwoord OV1). Hiertoe beschikt de AIVD over een aantal bevoegdheden. Hieronder vallen de zogenoemde 'bijzondere inlichtingenmiddelen', waarmee heimelijk informatie omtrent andere personen wordt verzameld. De agent is de belangrijkste van deze bijzondere inlichtingenmiddelen. Agenten zijn eigenlijk spionnen, en mogen in die hoedanigheid strafbare feiten plegen. Hiervoor gelden wel diverse regels, maar in de kern kan de agent straffeloos strafbare feiten plegen. Dit maakt dan ook dat de agent als verdachte in het vizier van

de politie kan komen. Indien een agent verdachte wordt, loopt hij het risico dat zijn identiteit bij de politie bekend wordt of dat de politie inzicht krijgt in de inlichtingentrajecten van de dienst en daarmee in diens informatiepositie. Bij aanhouding verliest de dienst ook een inlichtingenpositie. De AIVD wil dit alles ten alle tijden voorkomen, hetgeen een goede afstemming met de politie onontbeerlijk maakt.

C: HP-kenmerk 3: de intelligence-cyclus

De intelligence-cyclus is het vraaggestuurde werkproces van de inlichtingen- en veiligheidsdiensten en valt uiteen in de volgende fasen: (1) het vaststellen van de intelligence-agenda, (2) planning en opdracht, (3) verzamelen informatie, (4) verwerken, (5) analyseren, en (6) verspreiden van intelligence-producten. Wij hebben weinig zicht gekregen op de vierde en vijfde fase van de cyclus. Deze worden nauwelijks gereguleerd door de WIV 2002 en vinden plaats binnen de muren van de dienst. Vanwege de verregaande geheimhouding, is er weinig inzicht in de wijze van verwerking en analyse die de AIVD hanteert. De AIVD maakt echter wel gebruik van deze fasen (gedeeltelijk antwoord OV1). Dit is logischerwijs noodzakelijk: verzamelde informatie moet worden verwerkt en om tot een dreiginginschatting te komen, zijn analyses nodig. De meeste informatie die beschikbaar is, gaat over de fasen van informatieverzameling en verspreiding. De WIV 2002 geeft met betrekking tot deze fasen uitgebreide regels.

D: HP-kenmerk 4: de geheimhouding

De AIVD wordt gebonden aan een verregaande geheimhouding die is gecodificeerd in artikel 15 WIV 2002. Slechts in bepaalde gevallen is het de dienst toegestaan om af te wijken van deze geheimhouding. De geheimhouding van de dienst geldt met name ten opzichte van de buitenwereld. Om toch de in een democratische rechtsstaat noodzakelijke controle en toezicht te hebben, is er in Nederland een complex stelsel in het leven geroepen. De belangrijkste toetsing en controle vindt plaats door de Commissie van Toezicht. Daarnaast is er ook een parlementaire controle.

Onze slotconclusie voor dit hoofdstuk luidt als volgt: de AIVD voldoet aan alle kenmerken die in hoofdstuk twee genoemd worden. Het is daarmee een typische veiligheidsdienst.

In het volgende hoofdstuk behandelen wij de CIE op dezelfde wijze als wij in dit hoofdstuk de AIVD hebben behandeld.

4| De Criminele Inlichtingeneenheid

In dit hoofdstuk beantwoorden we OV1 vanuit het gezichtspunt van de politie. We doen dit door de traditionele LP-kenmerken van de politie verder uit te werken voor de Nederlandse situatie en ze te combineren met onze bevindingen betreffende de criminele inlichtingeneenheid (CIE). De CIE is binnen de politie exclusief belast met het verzamelen van inlichtingen afkomstig van informanten en heeft als taak het verkrijgen van inzicht in de zware en georganiseerde criminaliteit en terrorisme. Het is daarom één van de belangrijkste onderdelen van de politieorganisatie met betrekking tot de bestrijding van deze criminaliteitsvormen.

Het hoofdstuk begint met een overzicht van de historische ontwikkeling van de CIE (sectie 4.1). Vervolgens gaan wij in op de CIE in het algemeen en staan wij specifiek stil bij de taak en werkzaamheden van de CIE (sectie 4.2). Daarna gaan wij in op het werkproces van de CIE. Dit proces valt uiteen in drie elementen: (1) het verzamelen van inlichtingen door middel van het runnen van informanten (sectie 4.3), (2) het verwerken van de verzamelde inlichtingen (sectie 4.4) en (3) het verstrekken van de verwerkte inlichtingen (sectie 4.5). De werkprocessen van de CIE worden tot in detail gereguleerd door wet- en regelgeving, en daar gaan wij in de secties die het werkproces behandelen dan ook uitvoerig op in. Wij sluiten af met een hoofdstukconclusie (sectie 4.6).

4.1 Historische ontwikkeling CIE

Al lang voor het ontstaan van de moderne bureaucratische politie in de 18e eeuw maakten overheden gebruik van informanten die heimelijk informatie verstrekten over andere burgers, en de eerste 'lage politiediensten' namen dit gebruik over (zie Chapman 1970; Stove 2003; Andreas en Nadelmann 2006). De Nederlandse politie werd ten tijde van en na de Franse bezetting in 1806-1813 grotendeels gebaseerd op het Franse politiemodel van Fouché (zie Fijnaut 2006: 46 e.v.; zie ook hoofdstuk 2). Het is niet verwonderlijk dat de Nederlandse politie destijds gebruik maakte van het instrument van de informant, maar het duurde tot de tweede helft van de 20e eeuw voordat er min of meer specialistische politiële inlichtingenafdelingen ontstonden. Wij zullen ons hier echter beperken tot een korte beschrijving van de geschiedenis van de CIE. De complexe bredere geschiedenis van de Nederlandse politie zullen wij hier verder buiten beschouwing laten: we verwijzen hiervoor naar Fijnaut (2006).

De wijze waarop lange tijd met informanten en de criminele inlichtingen werd omgegaan, was grotendeels afhankelijk van de betreffende politieman. Van een eenduidige inlichtingenpraktijk was geen sprake. Dit veranderde in de jaren '60 van de vorige eeuw. Het werken met informanten werd destijds bij de grote politiekorpsen geïnstitutionaliseerd in specialistische afdelingen, Criminele Inlichtingendiensten (CID-en) genoemd. Deze diensten hadden als taak het onderhouden van contacten met informanten die hen informeerden over (potentiële) criminelen en criminaliteit. De informatieverzameling was met name zaaks- en resultaatsgericht: het verkregen inzicht kon worden gebruikt bij het opsporen en voorkomen van misdrijven (zie Aalbersberg, Barendregt en De Wit 1993: 52; Koelewijn 2009: 94). De CID-en waren in deze periode met name gericht op het ondersteunen van lopende opsporingsonderzoeken. Van opbouw van een informatiepositie als zelfstandige doelstelling was overigens geen sprake. Dit veranderde in de jaren '70 van de vorige eeuw. We behandelen de volgende periodes: (A) 1970 tot 1979, (B) 1980 tot 1987,

(C) 1988 tot 1993 en (D) 1994 tot 2001. De periode van 2001 tot heden zullen we in deze sectie niet apart behandelen: in deze periode vinden de ontwikkelingen plaats die voor ons onderzoek van groot belang zijn, zoals het islamitisch terrorisme en de ontwikkeling van IGP. Dit onderzoek behandelt daarom deze periode.

(*A) 1970 tot 1979*

In de jaren '70 van de vorige eeuw kwamen met de opkomende drugshandel voor het eerst echte georganiseerde criminele groeperingen in Nederland aan het licht. De voortschrijdende ontwikkeling van de criminaliteit vereiste van de rechercheafdelingen die waren belast met de opsporing van strafbare feiten dat zij zich in toenemende mate gingen professionaliseren.[162] Vanaf de jaren '70 kwamen er rechercheurs die zich in toenemende mate specialiseerden in de opsporing van de georganiseerde criminaliteit (zie voor een beschrijving van de moeizame professionalisering van de opsporing in het algemeen in deze periode: Fijnaut 2006: 843 e.v.). De georganiseerde criminaliteit vereiste een proactieve aanpak van de recherche, en het waren met name (doch niet enkel) de CID-en die experimenteerden met verschillende proactieve opsporingsmethoden (zie ook: Fijnaut 2006: 861-863). Het verzamelen van inlichtingen door middel van het runnen van informanten was één van de belangrijkste methoden van het CID-werk. Overigens werden de proactieve (niet in de wet geregelde) opsporingsmethoden, zoals observatie, infiltratie, en het doorlaten van verdovende middelen, ook al voordat er CID-en bestonden, toegepast (Van der Bel et al. 2009: 28). Het runnen van informanten was echter niet voorbehouden aan de CID: ook tactische rechercheurs runden informanten. De informatie van deze informanten werd daarnaast vaak als een soort persoonlijk eigendom gezien en onderling over het algemeen niet of nauwelijks gedeeld (Aalbersberg et al. 1993: 53).

De rechercheurs van de CID verschilden in een aantal opzichten van de andere politiemensen die contacten onderhielden met informanten. Allereerst specialiseerden zij zich met name in de georganiseerde criminaliteit en werden op dit onderwerp experts. Daarnaast was de CID binnen de politieorganisatie een geheimzinnige en schimmige organisatie: het was de 'sectie stiekem' van de politie. De CID-en hielden zich in eerste instantie met name bezig met het runnen van informanten, maar later gingen ze ook over tot het toepassen van andere opsporingsmethoden.

Omwille van de bronbescherming hielden de CID-ers de eigen werkzaamheden angstvallig verborgen voor de buitenwereld. Andere politieonderdelen (inclusief andere CID-en) waren doorgaans niet op de hoogte van de CID-activiteiten, maar ook het OM kreeg nauwelijks inzicht in het geheime CID-werk. De samenwerking tussen de CID-en onderling en de CID en andere bij de opsporing betrokken partijen had behoorlijk te lijden onder de zweem van geheimhouding die om de CID hing. Daarnaast zorgde deze geheimhouding ervoor dat de CID verborgen bleef voor kritische toetsing en controle van de eigen werkzaamheden. Het politiële inlichtingenwerk miste met name een juridische grondslag, maar vanwege onenigheid tussen het ministerie van Binnenlandse Zaken

[162] Dit proces van actie-reactie tussen de politie en de criminaliteit kent ook een psychologische component, namelijk *mirror-imaging*. Dit houdt in dat de politie aan georganiseerde criminaliteit bepaalde kenmerken toeschrijft die eigenlijk van toepassing zijn op de eigen organisatie. Het is voorstelbaar dat het proces van *mirror-imaging* steeds meer een rol is gaan spelen naarmate de politie zich meer richt op georganiseerde criminaliteit. In ons onderzoek zullen wij *mirror-imaging* echter niet verder behandelen.

en het ministerie van Justitie duurde het tot halverwege de jaren '80 voordat er regelgeving zou komen (Fijnaut 2006: 845). In de jaren '80 werd geprobeerd om meer lijn en structuur aan te brengen in de CID-wereld.

(B) 1980 -1987

De eerste CID-en verschilden onderling aanzienlijk van elkaar. Er was geen eenduidige taakstelling en een eenduidige structuur ontbrak (Van der Bel et al. 2009). Door middel van regelgeving probeerde men het CID-werk te structureren en professionaliseren. Zo moesten de taak en werkzaamheden van de CID in relatie tot andere onderdelen van de opsporing worden verduidelijkt. Tot aan het midden van de jaren '80 was het namelijk gebruikelijk dat ook rechercheurs van tactische opsporingsteams over informanten beschikten. Dit had tot gevolg dat er binnen de politiekorpsen parallelle en versnipperde informatieposities ontstonden. Het College van Procureurs Generaal wilde hier door middel van de regeling 'Tip-, Toon- en voorkoopgelden' verandering in aanbrengen. Dit was de eerste regelgeving ten aanzien van het CID-werk (Aalbersberg et al. 1993: 53). In de regeling kreeg de CID een centrale en coördinerende rol bij het inwinnen en verwerken van informanteninformatie. Het runnen van informanten werd steeds meer een CID-aangelegenheid.

In het begin van de jaren '80 werd bij de Centrale Recherche Informatiedienst (CRI) de Criminele Inlichtingen Centrale (CIC) opgericht (Aalbersberg et al. 1993: 53; Fijnaut 2006: 847 e.v.). De CIC had als doel om te komen tot een coördinatie van het CID-werk op een nationaal niveau. Zij ontwikkelde daartoe onder meer een standaard informatieformulier met behulp waarvan de CID-en onderling informatie konden uitwisselen. Het formulier bevatte een coderingssysteem voor de evaluatie van de betrouwbaarheid van de informanten (Aalbersberg et al. 1993: 53; Koelewijn 2009: 95). Deze ontwikkeling naar een meer landelijke afstemming en coördinatie van het criminele inlichtingenwerk paste overigens in het beleid vanaf het begin van de jaren '70 om de opsporing van zware vormen van criminaliteit piramidaal te organiseren, met eenheden op plaatselijk, regionaal en landelijk niveau (Fijnaut 2006: 847).

In 1985 werd er met het beleidsplan 'Samenleving en Criminaliteit' voor het eerst een specifiek beleid vastgesteld voor de aanpak van de georganiseerde criminaliteit (zie ook Fijnaut 2006: 940-941).[163] Een verdere professionalisering van de proactieve opsporingsmiddelen werd noodzakelijk geacht om de georganiseerde criminaliteit effectief te bestrijden. Omdat de georganiseerde criminaliteit zich niet aan de regionale grenzen hield, stelde het beleidsplan voor om een landelijke CID-structuur te ontwikkelen. Dit zou de samenwerking tussen de diensten verder stimuleren, hetgeen de bestrijding van de georganiseerde misdaad ten goede zou komen.

In 1986 werd deze structuur vastgelegd in de eerste CID-regeling met een bijbehorend privacy-reglement. De regeling bracht een onderscheid aan tussen lokaal, regionaal en landelijk niveau. De lokale CID was verantwoordelijk voor het plaatselijk inwinnen en verwerken van criminele inlichtingen. Zij deden het feitelijke runnen. De regionale CID had een verbindende, analyserende en coördinerende taak binnen de regio. De landelijke CID werd ondergebracht bij het CRI en kreeg als taak de internationale uitwisseling van inlichtingen en de coördinatie op landelijk niveau

[163] *Kamerstukken II* 1984/85, 18 995, nrs. 1-2.

(zie Koelewijn 2009: 96). Deze structuur kwam echter niet echt van de grond, onder meer omdat het uitwisselen van inlichtingen door het grootste deel van de CID-en werd gezien als een risico voor de bronafscherming. Daarnaast lagen de politiële organisatiestructuur en de primaire verantwoordelijkheid voor het politieoptreden destijds op gemeenteniveau (zie Fijnaut 2006 voor een uitgebreide historische analyse van de complexe organisatie van de Nederlandse politie). Dit was weinig bevorderlijk voor de beoogde uniformering en structurering van het CID-werk.

In deze eerste CID-regeling en het privacyreglement werd het proces van informatieverzameling geregeld en werden er regels gesteld omtrent de opslag, verwerking en verstrekking van criminele inlichtingen. Er werd een criterium voor de CID-subjecten gegeven: "*natuurlijke en rechtspersonen, ten aanzien van welke op grond van feiten en omstandigheden kan worden aangenomen dat zij als verdachte betrokken zijn, of naar redelijkerwijs kan worden vermoed betrokken zullen worden bij misdrijven die – gezien hun ernst of frequentie dan wel het georganiseerd verband waarin zij worden gepleegd - een ernstige inbreuk op de rechtsorde opleveren*" (artikel 1 sub c van het privacyreglement). Dit is de eerste begrenzing van het werkterrein van de CID (Aalbersberg et al. 1993: 55). De regeling formaliseerde ook de inmiddels gegroeide scheiding tussen de CID en de tactische opsporingsteams. De tactische opsporingsteams werden belast met het uitvoeren van de opsporingsonderzoeken, en werden daartoe ondersteund door de CID. Het runnen werd overgelaten aan de CID. Naast deze ondersteunende taak had de CID ook tot taak om een beter beeld van het criminele milieu te verkrijgen. De CID-regeling zei echter niets over de opsporingsmethoden die de CID hanteerde. Vanwege de nadruk op geheimhouding onttrokken de CID-en zich feitelijk grotendeels aan rechterlijke controle. Ook het OM had nauwelijks zicht op de activiteiten van de CID-en. De rechercheurs van de CID-en handelden grotendeels op eigen initiatief en schuwden innovatieve en verregaande methoden niet. Dit maakte dat de CID mogelijkheden had die de tactische teams niet hadden. Deze werden immers gecontroleerd door de rechterlijke macht. Van de CID werd in deze periode dan ook graag gebruik gemaakt omdat zij met oplossingen kwamen die voor anderen onmogelijk waren. In de praktijk kwam er van de beoogde uniformering van het CID-werk alsmede een toenemende samenwerking in de praktijk echter weinig terecht. In 1987 benoemden de ministers daarom een Begeleidingscommissie CID, die als doel had de politiële samenwerking op het gebied van criminele inlichtingen in het gehele land te bevorderen en te begeleiden. Daarbij diende onder meer aandacht besteed te worden aan (1) het toetsen van de bruikbaarheid van de CID-regeling en (2) het ontwikkelen van een adequate automatiseringsapplicatie (Aalbersberg et al. 1993: 56). In dezelfde periode werd de algemene bestrijding van georganiseerde criminaliteit prominent op de politieke agenda geplaatst door een eerste landelijke analyse van de georganiseerde criminaliteit, waarin werd geconcludeerd dat er ongeveer 200 criminele groeperingen in Nederland actief zijn. De informatie waarop de analyse was gebaseerd was door de regionale CID-en verzameld, en de analyse werd op landelijk niveau verricht door de CRI (Fijnaut 2006: 943). In hoofdstuk zeven zullen we zien dat de CIE anno 2012 nog steeds met problemen op beide gebieden kampt.

(C) 1988-1993

Aan het einde van de jaren '80 werd in het rapport 'Bedrijfsmatig Onderzoek Recherche' (IME Consult 1989) geconcludeerd dat (1) de CID te weinig klantgericht werkt, (2) de kwaliteit van de informatie tekort schoot omdat er weinig werd

nagedacht over de tactische haalbaarheid van onderzoeken en (3) de CID bij de andere rechercheteams nog steeds onbekend was vanwege de verregaande mate van geheimhouding. Inmiddels was in die periode bij diverse CID-en het besef gekomen dat de relatie met de afnemers van de informatie (de tactische opsporingsteams) diende te verbeteren. Er werd in die periode in toenemende mate geprobeerd om het contact met de tactische opsporingsteams beter te managen. Voorts trachtte men een cultuuromslag te bereiken. De CID moest meer informatie gaan verzamelen die de klant nodig heeft in plaats van zoveel mogelijk informatie te willen verzamelen (Aalbersberg et al. 1993: 60). In hoofdstuk zeven zullen we zien dat zowel de communicatie met andere diensten (het managen van de contacten) en een cultuuromslag terugkerende thema's zijn voor het criminele inlichtingenwerk.

Naar aanleiding van het hierboven genoemde rapport werden drie maatregelen genomen om wat aan de geconstateerde problemen te doen. De eerste maatregel was het samenstellen van een zwarte lijst van informanten die onbetrouwbaar waren gebleken. De tweede maatregel was het maken van afspraken over een centrale codering van informanten bij de landelijke CID. Hiermee probeerde men te voorkomen dat informanten die onbetrouwbaar waren gebleken in regio A vervolgens informant werden bij regio B. Daarnaast moest de code ervoor zorgen dat regio's niet dezelfde informanten runden, dit om dubbeltelling van informatie te voorkomen. De derde maatregel was het ontwikkelen van een landelijke verwijsindex waarin alle regionaal geregistreerde CID-subjecten waren opgenomen. Op deze manier was het mogelijk om vast te stellen of er bij verschillende CID-en informatie omtrent dezelfde subjecten aanwezig was, hetgeen de onderlinge uitwisseling van informatie zou kunnen stimuleren (Koelewijn 2009: 97).

Deze maatregelen bleken echter onvoldoende. Er waren drie knelpunten. Het eerste knelpunt vloeide voort uit het spanningsveld tussen bronafscherming en informatie-uitwisseling (Aalbersberg et al. 1993: 61). De CID-en probeerden hier onderling wat aan te doen door afspraken te maken over het gebruik van elkaars inlichtingen. Dit zou het onderlinge vertrouwen moeten versterken. Het tweede knelpunt betrof de neiging van de recherche om de CID-functie niet of slechts ten dele te gebruiken (Aalbersberg et al. 1993: 61). Vanwege de vereiste bronbescherming schermden de CID-en de eigen informatie en activiteiten af, hetgeen ertoe leidde dat de rechercheafdelingen op hun beurt de eigen informatiepositie voor de CID ging afschermen. Het beeld dat de tactische recherche van de CID had was vaak negatief en de informatiestromen bleven van elkaar gescheiden. In het verlengde hiervan ligt het derde knelpunt: de neiging van rechercheafdelingen om bepaalde tactische opsporingsonderzoeken in grote mate af te schermen van de buitenwereld, inclusief de CID, vanwege vermeende corruptie. Voor al deze belemmeringen geldt dat zij een effectief en efficiënt informatieproces (bestaande uit informatieverzameling, -coördinatie en analyse) in de weg staan (Aalbersberg et al. 1993: 62). Overigens werden enkele essentiële ingrediënten van de intelligencegestuurde politie (oftewel IGP, zie hoofdstuk vijf voor een inhoudelijke behandeling van dit concept) al in 1993 beschreven: "*wij zijn (…) van mening dat de zware en/of georganiseerde criminaliteit slechts adequaat bestreden kan worden, wanneer optimaal gebruik wordt gemaakt van de mogelijkheden tot integrale informatieverwerking en –analyse.*" (Aalbersberg et al. 1993: 63). In hoofdstuk vijf

gaan wij dieper in op IGP, en in hoofdstuk zeven behandelen wij in hoeverre de huidige CIE nog steeds te maken heeft met de hier genoemde belemmeringen.[164]

(D) 1994-2000

In de jaren '90 kwam de bestrijding van de zware en georganiseerde criminaliteit steeds prominenter op de Nederlandse politieke agenda. Voor de effectieve bestrijding van het complexe fenomeen van de georganiseerde criminaliteit was naast een regionale aanpak ook een bovenregionale aanpak nodig. De georganiseerde criminaliteit houdt zich immers niet aan regiogrenzen, dus de aanpak ervan zou dat ook niet moeten doen (zie Fijnaut 2006: 941 e.v.). Voor een goede beschrijving van de periode 1994-2000 nemen we een aanloop die begint aan het einde van de jaren '80.

Om de bovenregionale aanpak van de georganiseerde criminaliteit vorm te geven, werd eind jaren '80 onder meer het Interregionale Recherche Team Noord-Holland/Utrecht, oftewel IRT, opgericht. In het IRT werkten de politiekorpsen van Utrecht, Amsterdam-Amstelland, Gooi- en Vechtstreek, Noord-Holland Noord, Zaanstreek-Waterland en Kennemerland samen. De leiding over het IRT kwam in die periode in handen van het Utrechtse korps (zie Haenen 1996). Het IRT richtte zich op de top van de criminele netwerken en hanteerde daarbij een strikte geheimhouding ('*need to know*' benadering). Vanaf het begin van het IRT werd het team geplaagd door interne onderlinge conflicten. Met name de geheimhouding en de daarop volgende compartimentering leidden tot verstoorde verhoudingen (Haenen 1996: 34; Besse en Kuys 1997: 65-66). Daarnaast leek het erop dat leden van de Amsterdamse korpsleiding geen zelfstandige recherche-eenheid binnen het Amsterdamse ressort wensten die niet bereid was om zich te onderwerpen aan het primaat van de Amsterdamse recherche bij de aanpak van de zogenoemde Hollandse criminele netwerken (zie Besse en Kuys 1997: 63-66; zie ook Van de Bunt, Fijnaut en Nelen 2001: 60). Toch begon het IRT langzaam resultaten te boeken. In 1993 ging de leiding van het IRT over naar Amsterdam. In datzelfde jaar werden het IRT en de gemaakte afspraken met de regio's geconcretiseerd in een aantal convenanten tussen de ministers van justitie en binnenlandse zaken en de betrokken korpsbeheerders en hoofdofficieren van justitie.[165] Nog in 1993 zou Amsterdam echter de stekker uit het IRT trekken. De reden lag volgens Amsterdam in een opsporingsmethode waarvoor de Amsterdamse korpsleiding geen verantwoordelijkheid wenste te nemen (zie Haenen 1996).

De gewraakte methode is bekend geworden onder de namen 'groei informant', 'gecontroleerde doorlating' en 'Delta-Methode'(Van Traa 1996: 72 e.v.). De methode zou door de CID-Kennemerland zijn ontwikkeld (zie Besse en Kuys 1997), maar werd begin jaren '90 door diverse rechercheafdelingen in het hele land toegepast (Van Traa 1996: 72; Haenen 1996: 83-86). Het doel van de methode was om de top van een criminele organisatie in beeld te krijgen en te ontmantelen. De groei-informant van

[164] De ingrijpende politiële hervormingen die met de inwerkingtreding van de Politiewet in 1993 plaatsvonden, hebben onmiskenbaar ook invloed gehad op de CID-en in die tijd. In het kader van ons onderzoek is dit echter niet relevant, en wij zullen deze hervormingen dan ook buiten beschouwing.

[165] Een belangrijke afwezige bij het werk van de CID was tot aan de jaren '90 van de vorige eeuw de officier van justitie. Het OM ging zich pas aan het begin van de jaren '90 met het werk van de CID bemoeien. Bij de parketten die veel te maken hadden met de bestrijding van georganiseerde criminaliteit werden de eerste CID-officieren van justitie benoemd. Deze officieren bleken echter moeilijk te sturen, ook zij gingen uit van een strikte geheimhouding (zie Van der Bel et al. 2009: 30).

Kennemerland was betrokken bij het opzetten van sofdrugstransporten, en de regionale CID was hiervan op de hoogte. Door niet in te grijpen bij deze transporten, hoopte men dat de informant bekend zou komen te staan als iemand die betrouwbaar was en zodoende zou doorgroeien in het criminele milieu (zie ook Besse en Kuys 1997: 16-17; Van de Bunt et al. 2001). Toen deze manier van werken aan het licht kwam, brak er grote politieke onrust uit. Volgens de Amsterdamse politie was de politie dankzij het doorlaten van grote hoeveelheden drugs in feite verworden tot een groothandelaar in verdovende middelen, iets waarvoor de Amsterdamse korpsleiding zoals gezegd geen verantwoordelijkheid wenste te nemen (zie Besse en Kuys 1997; Van de Bunt et al. 2001: 1961). Uiteindelijk bleek dat ook de verantwoordelijke minister van justitie niet op de hoogte was van de tot dan toe succesvolle opsporingsmethoden. In Nederland werd kennelijk jarenlang een geheime methode toegepast waar slechts een aantal CID-ers en officieren van justitie van wisten, maar de uiteindelijke verantwoordelijken wisten van niets. In oktober 1993 werd het IRT ontbonden en kreeg de verantwoordelijke CID (Haarlem) de opdracht de burgerinfiltranten af te bouwen. Inmiddels werd de methode echter ook al toegepast in Rotterdam, en na een aantal andere incidenten en hardnekkige geruchten omtrent corruptie in het Amsterdamse korps, besloot het kabinet dat er een onafhankelijk onderzoek naar de ontbinding van het IRT plaats diende te vinden. De Commissie-Wieringa werd in het leven geroepen, hetgeen het begin was van een zeer roerige periode voor de opsporing van de zware en georganiseerde criminaliteit waarbij de relatie tussen de diverse betrokkenen in verregaande mate bekoeld raakte. Deze commissie stelde overigens vast dat de gehanteerde methoden niet onrechtmatig zijn toegepast, en dat de oorzaak van de IRT-affaire met name was toe te schrijven aan de opstelling van de top van de Amsterdamse politie (zie Van de Bunt et al. 2001: 61). Deze periode zou later de naam 'IRT-affaire' krijgen, en de gevolgen van deze affaire werken tot op de dag van vandaag door in het werk van de CIE-en, onder meer in de vorm van regelgeving.

Na de Commissie Wieringa en de daaropvolgende strafrechtelijke onderzoeken van onder andere de Rijksrecherche naar de Deltamethode (de zogenoemde Fort- en post-Fort-onderzoeken; zie Van de Bunt et al. 2001) werd er een Parlementaire Enquêtecommissie (PEC) in het leven geroepen om te onderzoeken hoe het zo ver had kunnen komen (Van Traa 1996; van de Bunt et al. 2001; Fijnaut 2006). De Commissie stelde een aantal problemen vast bij de bestrijding van de georganiseerde criminaliteit. Volgens de PEC was er sprake van een drieledige crisis in de opsporing, welke uit de volgende onderdelen bestond: (1) het ontbreken van normen (normeringcrisis), (2) een slecht functionerende opsporingsorganisatie (organisatiecrisis) en (3) een onduidelijke gezagsrelatie tussen het OM en de politie (gezagscrisis) (Van Traa 1996; zie ook Hoogenboom 2000: 4-5; Fijnaut 2006: 947; Corstens 2008: 258 e.v.; Van der Bel et al. 2009: 31).

De PEC stelde daarnaast vast dat de verschillende toepasselijke wettelijke regimes het geheel van regelgeving voor de politieorganisatie ondoorzichtig maakten. Ook de inrichting van de politieregisters waar onder andere de CID-en de verzamelde informatie in verwerkten, verschilde per korps. Informatie werd in de verkeerde registers opgeslagen en van verwijdering van gegevens uit de registers was nauwelijks sprake. Veel informatie-uitwisseling vond plaats via het *old-boys network*, hetgeen leidde tot ondoorzichtige en oncontroleerbare informatiestromen (Van Traa 1996: 283).

De PEC richtte zich ook meer specifiek op de CID (zie Van Traa 1996: 300-312). Aan de omgang met informanten die niet zelden zelf betrokken waren bij de

georganiseerde criminaliteit, kleven volgens de PEC grote gevaren. Er kunnen situaties ontstaan waarbij de rollen worden omgedraaid en men zich af kan vragen wie nu eigenlijk wie runt: de CID-er de informant of andersom (zie Van Traa 1996: 221)? De bovenstaande drieledige crisis had ook invloed op de CID. Voor de normeringcrisis en de gezagscrisis werden er specifiek binnen de CID-structuur oplossingen gezocht. Om de normeringcrisis aan te pakken, moest het werken met informanten meer worden gereguleerd en gecontroleerd en de verwerking en vastlegging van de informatie moest worden verbeterd (Van Traa 1996: 435). De gezagscrisis diende ook te worden opgelost: de vrijheid die de CID tot op dat moment had, diende te worden beperkt. De CID-officier van justitie moest een belangrijker controlerende rol krijgen bij zowel de administratieve afhandeling van contacten met informanten als bij de inhoudelijke gesprekken met de informanten (Van Traa 1996: 436-437). Er moest een evenwicht worden gevonden tussen de controle en verantwoording van de informatie en de bescherming van de identiteit van de informant. Dit leidde onder andere tot nieuwe regelgeving voor het werken met informanten en de gegevensverwerking door de CID (zie Kielman 2010: 34).

De organisatiecrisis kon niet specifiek voor de CID worden opgelost: dat vereiste een verandering van de gehele organisatie van de opsporing. Een belangrijke stap in de richting van het oplossen van de organisatiecrisis was de oprichting van de nationale recherche in 2005. Dat dit niet de organisatiecrisis op heeft gelost, blijkt uit de komende verregaande hervormingen van het politiebestel, te weten de ontwikkeling van de nationale politie. In 1995 werd de CID-regeling aangepast en werden er door politie en justitie nieuwe richtlijnen ingevoerd met betrekking tot de werkzaamheden van de CID en overige niet bij wet gereguleerde opsporingsbevoegdheden. De regeling trad op 1 november 2000 in werking. Het accent van het criminele inlichtingenwerk kwam primair te liggen op de informatieverwerking en informatievoorziening ten behoeve van de recherche. Dit werd ook verduidelijkt in de nieuwe naam van de dienst: Criminele Inlichtingeneenheid (CIE). De CIE is een onderdeel van de rechercheorganisatie, net zoals de andere rechercheonderdelen, en moet dan ook niet langer worden gezien als een zelfstandig onderdeel van de politieorganisatie. In 2000 trad ook de Wet Bijzondere Opsporingsbevoegdheden (Wet BOB) in werking. Deze wet reguleerde de tot dan toe toegepaste opsporingsmethoden en bracht deze onder de werking van het Wetboek van Strafvordering. De ontwikkelingen op het gebied van wetgeving leidden uiteindelijk tot een uitgebreid stelsel van wet- en regelgeving voor het criminele inlichtingenwerk. In dit hoofdstuk zullen wij deze wet- en regelgeving (voor zover relevant) uitgebreid behandelen.

4.2 De CIE in het algemeen

Van de CIE bestaat vaak het beeld dat zij de sectie stiekem is binnen de politie, de geheime eenheid waar vaak activiteiten worden ontplooid die de normale politie niet zijn toegestaan. Aan de ene kant klopt dit beeld: het is een onderdeel van de politieorganisatie waar geheimhouding en afscherming van de werkzaamheden een belangrijk deel uitmaken van het dagelijkse werk. Aan de andere kant klopt het beeld niet: de CIE is een onderdeel van de politieorganisatie en heeft zich zodoende aan alle wetten en regels die voor de politie in het algemeen gelden te houden. CIE-ers zijn ‘gewoon’ politieambtenaren en dienen overeenkomstig te handelen. Zo moet er bijvoorbeeld sprake zijn van een bepaalde transparantie. De werkzaamheden van de CIE worden zeer uitgebreid gereguleerd. In deze sectie bezien wij waarom de

politieorganisatie over zo'n eenheid beschikt (subsectie 4.2.1). Daarna beschrijven wij de taak van de CIE zoals beschreven in de relevante regelgeving (subsectie 4.2.2). De afscherming van de identiteit van de informant behandelen wij als een apart onderwerp, omdat dit één van de kernaspecten van het werk van de CIE is (subsectie 4.2.3). Wij sluiten de sectie af met een korte behandeling van de organisatie van de CIE (subsectie 4.2.4).

4.2.1 Waarom een CIE?

Informanten zijn onontbeerlijk voor de bestrijding van de zware georganiseerde criminaliteit. Het behoeft, denken we, nauwelijks uitleg dat het zijn van informant voor de betreffende persoon vaak levensgevaarlijk is. Vanwege dit (levens)gevaar dient de informant de garantie te krijgen dat zijn identiteit zoveel mogelijk geheim blijft. Daarnaast geldt dat als de politie onzorgvuldig omspringt met de geheimhouding van de identiteit van haar informanten, potentiële nieuwe informanten minder snel bereid zullen zijn om informant te worden. Dit heeft verregaande gevolgen voor de informatiepositie van de politie. Afscherming van de identiteit van de informant (geheimhouding) is dus van groot belang voor de CIE, maar hoe past dit binnen het algemene systeem van regelgeving van de opsporing?

Het voorgaande is voor de wetgever de reden geweest om een apart organisatieonderdeel met een eigen juridisch regime op te richten: de criminele inlichtingeneenheid (CIE). Dit juridisch regime wordt onder meer gevormd door:

(1) De Politiewet 1993[166]
(2) De WPG en het Bpolg[167]
(3) De CIE-regeling[168]
(4) De Instructie voor de CIE-officier van justitie[169]
(5) De Instructie CIE-registercontrole.[170]

In de volgende secties en subsecties zullen wij dieper ingaan op het juridisch regime van de CIE. We beginnen met de taakstelling en werkzaamheden van de CIE (volgens de CIE-regeling).

4.2.2 De taak en de werkzaamheden van de CIE

Zoals reeds aan bod is gekomen in de beschrijving van de historische ontwikkeling van de CIE (sectie 4.1), is de CIE het enige organisatieonderdeel van de politie dat door de wetgever belast is met het runnen van informanten (zie ook artikel 12 lid 7 WPG). Zowel binnen de politieorganisatie als bij de buitenwereld bestaat er echter vaak het beeld dat de CIE zich enkel en alleen bezighoudt met het runnen van informanten. Dit is een misverstand: de CIE-taak omvat veel meer dan het runnen van

[166] Politiewet 1993, Wet van 9 december 1993, Stb. 724, laatstelijk gewijzigd bij wet van 1 januari 2009, Stb. 2008, 281.
[167] Besluit van 14 december 2007, houdende bepalingen ter uitvoering van de Wet politiegegevens (Besluit politiegegevens), Stb. 550. De WPGWPG zullen wij in subsectie 4.5.1 kort toelichten.
[168] Regeling criminele inlichtingen eenheden, Stcr. 2000, 198 (CIE-regeling), laatstelijk gewijzigd op 28 januari 2009.
[169] Instructie CIE-officier van justitie (2006I002), 30 januari 2006.
[170] Instructie CIE-registercontrole (2007I003), 10 september 2007.

informanten. De taak van de CIE volgt uit artikel 2 van de CIE-regeling en luidt als volgt.

"*De CIE is belast met de informatievoorziening in het kader van de uitvoering van de politietaak voor zover het een aantal nader beschreven misdrijven betreft.*"

De CIE heeft binnen de politie dan ook de primaire rol voor het actief inwinnen en doorgeven van die gegevens die relevant zijn voor de bestrijding van de zware criminaliteit (Van de Bel et al. 2009: 100).

De CIE voert haar taak uit in de zogenoemde 'informatieve voorfase', ook wel proactieve fase genoemd.[171] Dit is de onderzoeksfase waarin informatie wordt verzameld om (1) een algemeen inzicht te verkrijgen in het fenomeen van de zware en georganiseerde criminaliteit en (2) vast te kunnen stellen of er tegen bepaalde personen of groeperingen een tactisch opsporingsonderzoek kan worden gestart (zie Kielman 2010: 37-38). Om deze algemene taak uit te voeren, verricht de CIE een aantal werkzaamheden die zijn beschreven in artikel 4 van de CIE-regeling. Deze werkzaamheden omvatten in ieder geval:

(1) het verzamelen en verifiëren van criminele inlichtingen;
(2) het verwerken van criminele inlichtingen in een bestand, als bedoeld in artikel 2, eerste lid, van de Wet politiegegevens;
(3) het bevorderen van het gericht inwinnen en aanvullen van criminele inlichtingen en andere gegevens die in het kader van de strafrechtelijke handhaving van de rechtsorde in aanmerking komen voor verwerking op grond van de Wet politiegegevens;
(4) het analyseren van criminele inlichtingen en het aan de hand daarvan:
1°. signaleren van criminaliteitsontwikkelingen, voorzover het betreft misdrijven als bedoeld in artikel 10, eerste lid, onderdeel a, van de Wet politiegegevens;
2°. periodiek verslag doen ten behoeve van criminaliteitsbeelden;
het ter beschikking stellen van criminele inlichtingen overeenkomstig artikel 10, vijfde lid, van de Wet politiegegevens.

Deze opsomming van werkzaamheden geeft aan dat de werkzaamheden van de CIE inderdaad meer omvat dan enkel het runnen van informanten of het verwerken van informatie afkomstig van informanten. Ook de definitie van het begrip 'criminele inlichtingen' onderstreept dit: criminele inlichtingen zijn 'gegevens, die in aanmerking komen voor verwerking op grond van artikel 10, eerste lid, onderdeel a, van de Wet politiegegevens'.[172] Dit betreft dus meer dan enkel de informatie afkomstig van een informant. De CIE heeft op basis van de CIE-regeling ook een belangrijke taak bij het verzamelen van bijvoorbeeld gegevens uit open bronnen voor zover deze in aanmerking komen voor verwerking in de zin van artikel 10 lid 1 sub a WPG.

Niet alle criminaliteitsgerelateerde gegevens komen dus in aanmerking voor verwerking in de zin van artikel 10 lid 1 sub a WPG. Zoals uit de taakstelling blijkt,

[171] Volgens Cleiren et al. (2007) is met de invoering van de wet BOB 'begripsmatig' de noodzaak vervallen om van een informatieve voorfase te spreken. De wet reguleert bepaalde bevoegdheden die voorheen in geheime trajecten werden toegepast en brengt de gehele opsporing onder het regime van strafvordering. De toepassing van opsporingsbevoegdheden is genormeerd en controleerbaar gemaakt (Cleiren et al. 2007: 9-10).
[172] Artikel 1 sub e Regeling criminele inlichtingen eenheden.

moet het gaan om een aantal nader beschreven misdrijven. In het CIE-jargon wordt gesproken over 'zwacri-informatie', maar wat is dit precies? De WPG stelt in artikel 10 lid 1 sub a WPG het hieromtrent het volgende.

"Politiegegevens kunnen gericht worden verwerkt met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij misdrijven:

"*1°. als omschreven in artikel 67, eerste lid, van het Wetboek van Strafvordering, die in georganiseerd verband worden beraamd of gepleegd en die gezien hun aard of de samenhang met andere misdrijven die in het georganiseerde verband worden beraamd of gepleegd, een ernstige inbreuk op de rechtsorde kunnen opleveren, of*

2°. waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld, of

3°. als omschreven in artikel 67, eerste lid, van het Wetboek van Strafvordering, die bij algemene maatregel van bestuur zijn aangewezen en die gezien hun aard of samenhang met andere door de betrokkene begane misdrijven een ernstige inbreuk op de rechtsorde opleveren;"

De CIE is dus bedoeld voor de zwaardere vormen van georganiseerde criminaliteit en niet voor de relatief 'lichtere' vormen van criminaliteit. Belangrijk is ook de analysetaak van de CIE. In de Memorie van Toelichting bij artikel 10 lid 1 sub a WPG wordt dit ook als de CIE-taak aangeduid.[173] Kort gezegd is de analyse van informatie omtrent de zware en georganiseerde criminaliteit een kerntaak van de CIE: geen ander onderdeel van de politie heeft een vergelijkbare (juridisch vastgelegde) taak. Op dit moment volstaat het om te concluderen dat de CIE-taak zowel het (coördineren van het) verzamelen van criminele inlichtingen omvat, alsmede de verwerking en de verstrekking van criminele inlichtingen, waarbij 'criminele inlichtingen' moeten worden gezien als informatie die betrekking heeft op de zware en georganiseerde criminaliteit. Dit is dus een aanzienlijk bredere taak dan enkel het runnen van informanten. In subsectie 4.4.3 zullen we dieper op de CIE-taak ingaan.

Het bovenstaande betekent overigens niet dat tactische opsporingsteams geen informatie met betrekking tot de zware en georganiseerde criminaliteit mogen verzamelen. Dit zou immers betekenen dat deze teams geen opsporingsonderzoeken kunnen uitvoeren op verdachten die deel uitmaken van de georganiseerde criminaliteit. Het grote verschil tussen deze informatieverzameling in het kader van een opsporingsonderzoek en de informatieverzameling door de CIE is de doelstelling van de informatieverzameling. De tactische opsporingsteams verzamelen informatie door middel van het toepassen van de opsporingsbevoegdheden uit het Wetboek van Strafvordering. Het doel van deze opsporingshandelingen is, kort gezegd, het verzamelen van bewijs en een uiteindelijke vervolging van een verdachte voor concrete strafbare feiten. Het doel van de informatieverzameling door de CIE is het opbouwen van een informatiepositie.[174] De CIE verzamelt dus informatie met als doel het verkrijgen van inzicht in de zware en georganiseerde criminaliteit (artikel 10 lid 1 sub a WPG). Dit gebeurt overigens doorgaans in een eerdere fase dan de tactische opsporing. De informatieverzameling door de CIE is het onderwerp van sectie 4.4. Voordat wij hier op ingaan, is het belangrijk om kort stil te staan bij een essentieel

[173] *Kamerstukken II* 2005/06, 30 327, nr. 3, p. 47.

[174] In elk CIE proces-verbaal wordt dan ook de volgende standaardtekst opgenomen: "*Dit proces-verbaal is niet bedoeld om te dienen als bewijsmiddel in een strafzaak.*"

onderdeel van de CIE-taak in de praktijk: de afscherming van de identiteit van de informant.

4.2.3 De afscherming van de identiteit van de informant

Uit de beschrijving van de geschiedenis van de CIE volgt al dat geheimhouding en bronbescherming essentiële onderdelen zijn van het CIE-werk. In deze subsectie staan wij kort stil bij deze geheimhouding.

De geheimhouding wordt *grosso modo* op drie manieren bereikt. Allereerst door fysieke beveiliging. De CIE-regeling stelt zware eisen aan de beveiliging van de CIE-informatie. Zo moet de ruimte zijn afgeschermd, mogen bezoekers niet zonder begeleiding door CIE-ruimtes lopen en dient het hoofd CIE zorg te dragen voor een adequate beveiliging van de informatiesystemen (artikel 11 CIE-regeling). De tweede wijze van afscherming is het uitgebreide systeem van autorisaties dat door de WPG wordt gehanteerd: de relevante politiegegevens worden slechts ter beschikking gesteld aan die medewerkers die de betreffende gegevens nodig hebben voor het uitvoeren van hun taak (zie sectie 4.5 voor een uitgebreide behandeling van dit systeem). De derde wijze van afscherming heeft te maken met het onderzoek ter terechtzitting en de rol die medewerkers van de CIE in het strafproces hebben. Dit speelt pas laat in het opsporingsproces, namelijk wanneer de behandeling van de strafzaak tegen een verdachte reeds is aangevangen (het onderzoek ter terechtzitting). In principe valt dit onderwerp buiten de scope van dit onderzoek, maar wij zullen er toch kort bij stilstaan omdat het een cruciaal onderdeel is van de voor de CIE vitale geheimhouding.

Tijdens het onderzoek ter terechtzitting kan de verdediging een zogenoemde 'rechtmatigheidsgetuige' oproepen waarmee zij probeert de rechtmatigheid van het optreden van de CIE en vaak ook de betrouwbaarheid van de informant of diens informatie in twijfel te trekken (zie Van der Bel et al. 2009: 244 e.v.). Deze getuige is een persoon die iets kan vertellen over de gang van zaken bij de betreffende CIE. In de regel is dit de CIE-chef, maar het komt ook voor dat de teamleider, de runner of in uitzonderlijke gevallen de informant zelf wordt gehoord. Medewerkers van de CIE of de CIE-officier van justitie zullen echter weinig loslaten over CIE-activiteiten. In de praktijk wordt in dit opzicht vaak gerefereerd aan een zogenoemde 'CIE-status'. Hiermee wordt gedoeld op een soort verschoningsrecht van een CIE-medewerker tijdens een onderzoek ter terechtzitting. Juridisch bestaat dit echter niet.[175] Wel heeft de rechter op basis van artikel 187b/293 Sv de mogelijkheid om antwoorden op vragen van de zijde van de verdediging aan het adres van de CIE-er die ter terechtzitting moet getuigen te beletten, indien het beantwoorden van die vragen een slagvaardige opsporing in gevaar brengt. Zo'n situatie doet zich voor als de veiligheid van een informant en mogelijk andere bij de opsporing betrokkenen wordt bedreigd.[176] In de praktijk wordt door de verhorende rechter zeer regelmatig, op basis van het afschermingsbelang, het beantwoorden van vragen belet (zie Van der Bel et

[175] Zie voor het algemene verschoningsrecht: artikel 218 WvSv. Dit artikel regelt de verschoning vanwege een geheimhoudingsverplichting die voortvloeit uit stand, beroep of ambt.

[176] Zie onder meer: HR 5 oktober 1982, NJ 1983, 297. Het betrof een informant die strafbare feiten had uitgelokt en uiteindelijk zelf verdachte werd. Hij deed dit vanwege het vooruitzicht van de beloning die hem van overheidswege werd verstrekt en kon dit doen omdat de controle van de CIE voorafgaand aan het plegen van die uitlokking tekort schoot. Ondanks alle aanwijzingen vond ook achteraf geen controle door de CIE en OM plaats. De wijze waarop het OM en de CIE in deze zaak hebben gehandeld, raakt volgens het Hof de integriteit van de overheid. Nu dit noch door de CIE noch door het OM werd onderkend, heeft het Hof om zowel de CIE als het OM te doordringen van de ernst van de situatie, het OM niet-ontvankelijk verklaard. Zie echter ook HR 07 december 2012, LJN: BU6784.

al. 2009: 186).[177] Het niet beantwoorden van vragen ter terechtzitting is echter geen recht van een individuele politiemedewerker, maar een mogelijkheid waar de rechter al dan niet gebruik van kan maken.[178] In de praktijk zullen de medewerkers van de CIE of de CIE-officier van justitie weigeren om op vragen van de verdediging antwoord te geven, indien zij van mening zijn dat de bronafscherming in gevaar komt. Dit kan uiteindelijk leiden tot een strafvorderlijke sanctie door de rechter.[179]

4.2.4 Organisatie

Wij behandelen in deze subsectie twee elementen van de organisatie van de CIE. Allereerst (A) de interne organisatie: welke functies zijn er binnen de CIE? Vervolgens (B) behandelen wij kort het OM, en gaan wij in op de verschillende officieren van justitie die bij het CIE-werk betrokken kunnen zijn.

A: De interne organisatie

We gaan eerst in op de vraag: welke functies kent de CIE? Een CIE bestaat in het algemeen uit een chef, een plaatsvervanger, één of meer teamleiders (ook wel coaches of begeleiders genoemd) en runners (Van der Bel et al. 2009: 131). De runners zijn de rechercheurs die zijn belast met het onderhouden van contacten met informanten. Daarnaast kennen de meeste CIE-en analisten en in sommige gevallen administratieve ondersteuning, zoals documentalisten. Het verschilt per korps hoe de CIE precies is opgebouwd. De CIE van de Dienst Nationale Recherche (DNR) heeft een zogenoemde *Back Office*, waar een aanzienlijk aantal analisten en andere medewerkers als administratieve ondersteuning is ondergebracht. Amsterdam-Amstelland heeft ook een eigen informatieafdeling, zij het dat deze kleiner in omvang is. De meeste CIE-en moeten het echter stellen met één of twee operationele analisten en administratieve ondersteuning.

Strategische analyse is in de meeste gevallen geen onderdeel van de CIE. Op het moment van schrijven (augustus 2011) waren er in het hele land slechts drie strategisch analisten bij verschillende CIE-en actief. Veel CIE-en die zijn ondergebracht bij een zogenoemde Regionale Informatie Organisatie (RIO) hebben weliswaar zelf weinig tot geen analisten in dienst, maar gebruiken op projectbasis analisten van de RIO.

B: Het OM

De officier van justitie maakt formeel geen deel uit van interne organisatie van de CIE, maar hij heeft een belangrijke rol bij de sturing en controle van de CIE. Wij zullen hier kort de verschillende officieren van justitie behandelen waarmee de CIE

[177] Zie HR 18 mei 1999, LJN: ZD1555, waarin het hof het beantwoorden van bepaalde vragen heeft belet omdat de antwoorden op die vragen zouden kunnen leiden tot het bekend worden van de identiteit van de informant hetgeen een risico voor diens veiligheid zou kunnen opleveren.

[178] Weigert een politieambtenaar alsnog een door de rechter toegestane vraag te beantwoorden, dan kan dit leiden tot niet-ontvankelijkheid van het OM.

[179] Zie bijvoorbeeld: Gerechtshof 's Gravenhage, 26 juni 2007, LJN: BA8168. Overigens wordt in veel van de gevallen waarbij de verdediging aanvoert dat het onrechtmatige handelen van de CIE of diens officier bestaat uit de schending van bijvoorbeeld de CIE-regeling of andere niet-strafvorderlijke bepalingen de *Schutznorm* gehanteerd: de handelingen leveren geen schending op van een norm die strekt tot bescherming van de belangen van de verdachte (zie HR 9 december 2003, LJN: AM0241; Van der Bel et al. 2009: 96-98).

tijdens haar werkzaamheden te maken kan krijgen. Het gaat om (1) de CIE-officier, (2) de recherche-officier, (3) de zaaks-officier en (4) de informatie-officier. Dit onderzoek gaat echter specifiek over de politieorganisatie, en wij zullen bij de behandeling van de officieren van justitie kort zijn.

De CIE-officier is belast met de controle op het runnen van informanten alsmede de rechtmatigheid en kwaliteit van de CIE-informatie. Op basis van artikel 13 Politiewet 1993 oefent de CIE-officier van justitie het gezag uit over de onder hem ressorterende CIE. Hij is daarbij gebonden aan de Instructie voor de CIE-officier van justitie. De CIE-officier van justitie valt functioneel onder de rechercheofficier van justitie en legt aan hem dan ook verantwoording af. Daarnaast fungeert de rechercheofficier ook als vraagbaak en sparringspartner van de CIE-officier van justitie (zie Van der Bel et al. 2009: 133).

Een andere officier met wie de CIE-officier te maken heeft, is de zaaksofficier: de officier van justitie die is belast met het gezag over een concreet opsporingsonderzoek. In de onderlinge relatie tussen de CIE-officier en de zaaks-officier wordt gestreefd naar zoveel mogelijk openheid. Met name daar waar het gaat om de wijze van het runnen van informanten moet de zaaks-officier op de hoogte zijn van relevante CIE-activiteiten. Hij is immers volledig verantwoordelijk voor alle opsporingsactiviteiten die in een specifieke zaak zijn verricht, en daartoe behoren ook de activiteiten van de CIE. Overigens blijft de identiteit van de informant in de regel voor de zaaks-officier afgeschermd.

De laatste jaren verschijnt er een nieuw soort officier van justitie die een rol krijgt op het gebied van het informatiewerk van de politie: de informatie-officier. Ontwikkelingen als IGP maken dat het informatieproces van de politie een steeds belangrijkere rol krijgt binnen de opsporing. Voorheen was de CIE-officier verantwoordelijk voor het informatieproces bij de politie: dit was ook opgenomen in de instructie voor de CIE-officier. In 2002 is deze gezagsrol met betrekking tot het informatiewerk uit de instructie verdwenen, maar inmiddels wordt deze dus door de informatie-officier vervuld (zie Van der Bel et al. 2009: 132). De informatie-officier richt zich met name op het zogenoemde ‘intake- en preweegproces’ (zie Van der Bel et al. 2009: 132). Hiertoe behoort bijvoorbeeld het inventariseren van criminele samenwerkingsverbanden (CSV’s) en het opstellen van werk- en projectvoorbereiding (het voorbereiden van uit te voeren opsporingsonderzoeken, onder andere door van tevoren doelstellingen en de haalbaarheid daarvan te benoemen). Welke taken precies tot het domein van de CIE-officier behoren en welke tot dat van de informatie-officier, moet in de praktijk nog worden uitgewerkt. Bepaalde parketten, zoals het Landelijk Parket, dat het bevoegd gezag uitoefent over de DNR, hebben de rol van CIE-officier en informatie-officier verenigd in één officier. In deze gevallen is de CIE-officier dus ook de informatie-officier, hetgeen in ieder geval recht doet aan de CIE-taak zoals in wet- en regelgeving is vastgelegd (zie subsectie 4.3.2).

4.3 Verzamelen

De CIE verzamelt informatie door middel van het runnen van informanten. Vergeleken met de AIVD wordt het runnen van informanten door de CIE (met name sinds de hierboven behandelde IRT-affaire) zeer uitgebreid gereguleerd. In deze sectie behandelen wij met name de juridische aspecten van het verzamelen van inlichtingen door de CIE en stippen wij kort aan waar de verschillen met de AIVD zitten. Als eerste komt het runnen van informanten op basis van de algemene taakstelling van

artikel 2 Politiewet aan bod (4.3.1). Vervolgens behandelen wij de figuur van de burgerinformant in de zin van artikel 126v WvSv (4.3.2). Hierna behandelen wij de informant als verdachte (4.3.3). Vervolgens behandelen wij in het kort het runnen in de praktijk (4.3.4). Wij sluiten de sectie af met het beantwoorden van de vraag of het runnen van informanten ook door anderen dan de CIE kan worden gedaan (4.3.5).

4.3.1 Juridische basis: artikel 2 Politiewet

Het verzamelen van politiegegevens door de CIE vindt voornamelijk plaats door middel van het runnen van informanten op basis van het taakstellende artikel 2 Politiewet 1993. Onder runnen wordt verstaan het onderhouden van contact met informanten. Een informant is '(een) persoon die heimelijk aan een opsporingsambtenaar informatie verstrekt omtrent strafbare feiten of ernstige schendingen van de openbare orde, die door anderen zijn of worden gepleegd of verricht, welke verstrekking gevaar voor deze persoon of voor derden oplevert.', aldus artikel 12 lid 7 WPG.[180] Iemand is dus al vrij snel informant in de zin van de WPG.

In de praktijk is het gewoon dat men pas van informanten spreekt indien deze zijn geregistreerd bij de CIE als informant (dat wil zeggen dat ze zijn ingeschreven in het informantenbestand van de CIE). Registratie als informant is belangrijk omdat de CIE slechts informatie kan verstrekken die afkomstig is van ingeschreven informanten (zie voor verstrekkingen door de CIE sectie 4.6). Informanten worden slechts ingeschreven als geregistreerde informant indien de CIE-officier daarvoor (en voor het runnen van de informant) toestemming heeft gegeven. Ook de informant zelf moet hiermee instemmen. Dit betekent dat de CIE er zorg voor dient te dragen dat de potentiële geregistreerde informant weet wat het zijn van informant betekent en welke regels er voor hem gelden. Deze spelregels worden met hem besproken en hij dient aan te geven de regels te begrijpen (Van der Bel et al. 2009: 137). Voorbeelden van deze spelregels zijn het verbod om te verklaren over strafbare feiten waarbij de informant zelf betrokken is en het verbod om met andere inlichtingendiensten te spreken dan de CIE. Dit laatste is van belang omdat als een informant bijvoorbeeld aan zowel de CIE als de AIVD informatie verstrekt en deze organisaties niet van elkaar weten wie de informant is, het erop kan lijken alsof de informatie van meerdere informanten afkomstig is. Deze dubbeltelling van informatie kan leiden tot onjuiste inschattingen en beslissingen door de politie en/of de AIVD. De AIVD kent deze regel overigens niet. Een informant of agent van de AIVD kan dus ook met andere inlichtingendiensten dan de AIVD praten. In de CIE-praktijk wordt er veel gewicht gehangen aan het met de informant doorlopen van de spelregels. In sommige regio's wordt er zelfs van de informant verwacht dat hij schriftelijk akkoord gaat met deze regels.

Indien een informant wordt geregistreerd, krijgt hij een unieke persoonscode (ICS-code, ICS staat voor Informanten Coderings Systeem). Met behulp van de code wordt gecontroleerd of een informant niet door verschillende CIE-en tegelijk wordt gerund om zo dubbeltelling van informatie te voorkomen. Daarnaast wordt er gekeken of de informant niet voorkomt in lopende opsporingsonderzoeken (dit gaat door middel van het zogenoemde Verwijsindex Recherche Onderzoeken en Subjecten, oftewel VROS) (zie Van der Bel et al. 2009: 137-138).

[180] Zie voor een korte toelichting van de WPG subsectie 4.5.1.

In het informantenbestand van de CIE wordt een onderscheid gemaakt tussen (1) de hiervoor genoemde geregistreerde informant, (2) de voorlopig geregistreerde informant, (3) de uitgeschreven informant en (4) gesprekscontacten. Een voorlopig geregistreerde informant is iemand waarmee wel gesprekken worden gevoerd, maar waarvan nog niet duidelijk is of hij informant kan of wil worden. Dit kan zo zijn omdat de CIE-officier eerst de kwaliteit van de informant moet beoordelen. Daarnaast is het ook mogelijk dat de informant zelf nog niet heeft aangegeven dat hij geregistreerd wil worden. De uitgeschreven informant is iemand die vanwege verschillende redenen (het woord zegt het al), uitgeschreven wordt. Het kan zijn dat de informant geen relevante informatie meer kan verstrekken over zware en georganiseerde criminaliteit, terrorisme daarbij inbegrepen, of dat de informant zich niet aan de afspraken met de CIE heeft gehouden of op een andere wijze onbetrouwbaar is gebleken (zie ook Van der Bel et al. 2009: 138). In het laatste geval kan de informant op de 'zwarte lijst' worden geplaatst: deze informanten mogen niet meer worden gerund (Van Traa 1996: 206).

Als vierde categorie noemen wij nog de gesprekscontacten. Dit zijn mensen die een specifieke kennis hebben omtrent specialistische onderwerpen. Het gaat dan bijvoorbeeld om wetenschappelijke onderzoekers of andere experts, maar bijvoorbeeld ook om mensen die in een bepaalde buurt wonen of horecagelegenheden bezitten. De CIE gaat met deze mensen gesprekken aan om advies te krijgen omtrent bepaalde onderwerpen. Het gaat in deze gevallen niet om informanten (geregistreerd of voorlopig geregistreerd): de CIE kan met deze personen alleen spreken over algemene, niet tot specifieke personen of strafbare feiten te herleiden onderwerpen. Als het gesprek met een gesprekscontact wel leidt tot criminele inlichtingen die te herleiden zijn tot personen of specifieke strafbare feiten, dan kan de CIE in eerste instantie niets met de informatie doen. Indien de CIE de informatie toch wenst te verstrekken, dan zal het gesprekscontact eerst toestemming moeten geven en met de regels akkoord gaan om vervolgens (met toestemming van de CIE-officier) ingeschreven te kunnen worden als (voorlopig) geregistreerde informant.

Het feit of iemand ingeschreven is als informant is in het kader van de WPG overigens niet doorslaggevend bij de beoordeling of iemand informant is of niet. De persoon die nog niet staat ingeschreven als informant, maar waarmee al wel gesprekken zijn gevoerd, krijgt dezelfde bescherming als die de geregistreerde informant toekomt. Ook deze personen vallen onder de reikwijdte van artikel 12 WPG.

4.3.2 Juridische basis: artikel 126v WvSv

In het voorgaande hebben wij gesteld dat de juridische basis voor het runnen van informanten artikel 2 Politiewet is. Er is echter nog een andere juridische grondslag mogelijk voor het runnen van informanten: artikel 126v/126zt WvSv.

Sinds de invoering van de wet BOB in 2000 zijn er discussies binnen de CIE omtrent de eventuele toepasbaarheid van artikel 2 Politiewet 1993 op het runnen van informanten. De vraag die rijst is kortweg of de inzet van een informant een meer dan beperkte inbreuk maakt op de persoonlijke levenssfeer van degene over wie de informant verklaart. Indien dit het geval is, biedt artikel 2 Politiewet 1993 onvoldoende grondslag om informanten te runnen. Dit artikel maakt immers slechts een beperkte inbreuk op de persoonlijke levenssfeer mogelijk (zie Corstens 2008: 274 e.v.). Indien er sprake is van een meer dan beperkte inbreuk, dan biedt artikel 126v WvSv grondslag met betrekking tot de 'commune criminaliteit', en artikel 126zt

WvSv voor de terroristische misdrijven. Artikel 126v kan worden toegepast tegen een verdachte of degene ten aanzien van wie een redelijk vermoeden bestaat dat hij is betrokken bij het in georganiseerd verband beramen of plegen van misdrijven. Artikel 126zt WvSv maakt het al mogelijk om bij aanwijzingen van een terroristisch misdrijf stelselmatig informatie in te winnen omtrent een persoon, aldus lid 1 sub b van dat artikel (zie ook: Corstens 2008: 460).

Uit het gegeven dat artikelen 126v en 126zt WvSv in de wet BOB zijn geplaatst, volgt dat deze artikelen slechts kunnen worden toegepast in het kader van een opsporingsonderzoek, dat wil zeggen een onderzoek met het oog op het nemen van een strafvorderlijke beslissing (zie artikel 132a WvSv). CIE-ambtenaren zijn opsporingsambtenaren in de zin van artikel 141 aanhef en onder b WvSv jo. artikel 3 lid 1 onder a en c Politiewet 1993. Ze zijn net als andere opsporingsambtenaren belast met de opsporing van strafbare feiten. Dit betekent dat zij kunnen beschikken over dezelfde opsporingsmiddelen en -bevoegdheden als andere opsporingsambtenaren. Er staat een runner van de CIE dus formeel juridisch niets in de weg om een opsporingsbevoegdheid als artikel 126v of 126zt WvSv toe te passen. Er zijn echter wel andere bezwaren aan te dragen. De door de inzet van artikel 126v verzamelde informatie kan namelijk worden gezien als bewijs, en bewijsmateriaal moet tijdens het onderzoek ter terechtzitting getoetst kunnen worden (Van der Bel et al. 2009: 140). Deze toetsing kan vervolgens betekenen dat de 126v-burger verplicht kan worden om een getuigenis af te leggen, waarmee diens rol als informant en identiteit bekend worden. Dit is voor CIE-chefs en CIE-officieren een belangrijke reden om geen gebruik te maken van de mogelijkheid van artikelen 126v en 126zt. Bronbescherming is dus het belangrijkste bezwaar tegen het gebruik van deze artikelen (zie Beijer 2004: 89; Van der Bel et al. 2009: 143).

In de praktijk bestaat er onduidelijkheid over de verhouding tussen de gewone informant die op basis van artikel 2 Politiewet 1993 wordt gerund, en de 126v/126zt-burger. De wetgever is er kennelijk van uitgegaan dat er een verschil tussen beide figuren is, maar hoe dat in de praktijk uitwerkt, heeft van de wetgever weinig aandacht gekregen (zie ook Van der Bel et al. 2009: 142). Of artikel 2 Politiewet 1993 voldoende grondslag biedt of dat er overgegaan dient te worden tot de inzet van 126v danwel 126zt WvSv, wordt bepaald aan de hand van de vraag of de inbreuk op de persoonlijke levenssfeer van de verdachte meer dan beperkt is.[181] Indien de inbreuk meer dan beperkt is, is er sprake van een stelselmatige informatieverzameling door middel van een burgerinformant. De bijzondere opsporingsbevoegdheden van 126v of 126zt bieden dan de grondslag voor de inzet van de burgerinformant, en niet artikel 2 Politiewet 1993. Wij staan als eerste kort stil bij (A) het begrip stelselmatigheid en de invulling hiervan door de wetgever. Vervolgens (B) behandelen wij de twee benaderingen van stelselmatigheid die in de praktijk door de CIE en het OM worden gehanteerd, te weten (1) de mate van sturing en (2) in hoeverre een beeld van iemands persoonlijke levenssfeer wordt verkregen. Als laatste gaan wij in op (C) de andere zienswijzen die mogelijk zijn.

A: Stelselmatigheid

Voor het beantwoorden van de vraag of er sprake is van een stelselmatige informant (waarvoor artikel 126v en 126zt WvSv de grondslag bieden) moet worden bezien of er met de informatie van de informant een min of meer compleet beeld van een

[181] Zie HR 19 december 1995, NJ 1996, 249.

subject wordt verkregen. Het gaat met andere woorden om in hoeverre de mogelijke inbreuk op de persoonlijke levenssfeer van een subject meer dan beperkt is (zie Kielman 2010). Er zijn echter geen concrete eisen om te beoordelen of dit het geval is, en verschillende zienswijzen zijn mogelijk. De wetgever biedt wel een aantal aanknopingspunten.[182]

In een brief aan de Tweede Kamer stelt de toenmalige Minister van Justitie met betrekking tot de stelselmatigheid dat het van belang is dat er een min of meer volledig beeld kan worden verkregen van bepaalde aspecten van iemands leven. Bepalend hierbij is de opdracht aan de informant en het resultaat dat vooraf redelijkerwijs door de inzet van de informant kan worden verwacht (Beijer et al. 2004: 90). Het gaat er dus om in welke mate de politie de informant heeft gestuurd en of politie en justitie, voordat ze met de informant spraken, konden verwachten dat de informatie een min of meer compleet beeld van bepaalde aspecten van het leven van een subject zou opleveren. Dit laatste betekent dat het mogelijk is dat een informant achteraf veel meer heeft verteld dan van tevoren ingeschat kon worden en dat daarmee een min of meer compleet beeld van het privéleven van een subject is verkregen, maar dat er niet aan de eisen van artikel 126v WvSv (of 126zt) behoefde te worden voldaan. Immers, het was vooraf redelijkerwijs niet goed in te schatten.

B: Twee benaderingen door de CIE en het OM

Tijdens de evaluatie van de wet BOB kwamen er twee benaderingen van stelselmatigheid naar voren die binnen de CIE en het OM leefden. De eerste benadering acht de mate van sturing bepalend voor het vaststellen of er sprake is van stelselmatigheid, de tweede benadering focust op de vraag of er min of meer een compleet beeld van het leven van een subject wordt verkregen (Beijer et al. 2004). Volgens de hiervoor reeds aangehaalde brief van de minister zijn dit echter niet twee verschillende visies, maar is de eerste (sturing) een onderdeel van de tweede (kort gezegd privacy). Beide benaderingen zijn in dat opzicht juist, maar te beperkt. Voor de beoordeling van stelselmatigheid kan namelijk in voorkomende gevallen de cumulatie van de mate van sturing en het resultaat dat men van tevoren redelijkerwijs mocht verwachten van belang zijn. Dit is een bestanddeel van het criterium 'min of meer een volledig beeld verkrijgen van aspecten van iemands leven'.

Het Landelijk Platform CIE-officieren (LPC) stelt hieromtrent dat van belang is (1) de positionering van de informant ten opzichte van het subject van het onderzoek en (2) de mate van sturing door de politie van activiteiten van de informant (Van der Bel et al. 2009: 142-143).[183] Bij de vraag hoe de informant is gepositioneerd ten opzichte van het subject gaat het met name om de vraag of de informant zich begeeft in een omgeving waarin de potentiële verdachte mag veronderstellen zichzelf te kunnen zijn, oftewel de binnenste privékring. Indien informatie uit die binnenste privékring wordt verzameld, dan is er sprake van een meer dan beperkte inbreuk op de privacy (Van der Bel et al. 2009: 144). Vervolgens moet nog worden bezien in hoeverre de CIE heeft gestuurd op het verzamelen van de informatie. Met andere

[182] Zie voor een behandeling van de relevante jurisprudentie Van der Bel et al. 2009: 148 e.v.

[183] De vraag die nu rijst, is hoe dit in de praktijk uitpakt. Wanneer is er sprake van actieve politiebemoeienis? In de praktijk zullen runners aan een informant gericht vragen stellen, en uit die vragen valt door de informant af te leiden in welke subjecten of onderwerpen de CIE geïnteresseerd is. De kans is dan groot dat zij zich hierdoor laten sturen. Het is echter niet goed na te gaan of de runners de vragen gebruiken om te sturen. We zullen hier derhalve niet langer bij stil staan, omdat deze vraag buiten de scope van ons onderzoek valt.

woorden: is er sprake geweest van actieve politiebemoeienis, bijvoorbeeld door de informant gericht informatie in te laten winnen op een bepaalde persoon of (veronderstelde criminele) groepering? Van deze twee visies is de dominante visie dat het met name gaat om de mate van sturing. Er moet aan allebei de eisen worden voldaan, wil er sprake zijn van een stelselmatige toepassing van een bevoegdheid die een specifieke wettelijke grondslag vereist. Op zichzelf is deze visie niet echt verrassend: sturing is immers het aspect waar het OM en de CIE-leiding de meeste invloed en controle op kunnen uitoefenen. De runners worden dan ook geïnstrueerd de informant zo weinig mogelijk te sturen.

C: Twee andere zienswijzen

Naast de bovenstaande zienswijzen zijn er ook nog andere zienswijzen mogelijk. Wij noemen er twee. Zo stelt Van Straelen (2002) dat er voor de beoordeling van stelselmatigheid drie criteria van belang zijn, te weten (1) de aard van de informatie, (2) de verwachting van een subject omtrent zijn persoonlijke levenssfeer (vergelijk het hierboven genoemde eerste criterium van het LPC) en (3) de mate van indringendheid van het inlichtingenwerk. Het eerste criterium houdt in dat informatie die een compleet beeld geeft van verschillende aspecten van het leven van een subject, al snel leidt tot een meer dan beperkte inbreuk op de persoonlijke levenssfeer. Er is dan sprake van een stelselmatige inwinning van informatie. Met betrekking tot het tweede criterium doelt van Straelen op het gegeven dat bijvoorbeeld een drugsdealer vanwege zijn strafbare handelen er rekening mee dient te houden dat hij in het beeld komt van politie en justitie en dat dit ertoe leidt dat er een inbreuk op zijn persoonlijke levenssfeer kan worden gemaakt: het is een soort beroepsrisico. De wijze waarop de informant aan diens informatie komt en de indringendheid van diens handelen vormen het derde criterium (Koelewijn 2009: 105).

De tweede zienswijze is van Corstens (2008: 459-460), die meent dat ook de aard van het contact tussen de runners en de informant van belang is. Indien er permanent en langdurig gebruik wordt gemaakt van de welwillende diensten van een burger, valt stelselmatigheid daaraan niet te ontkennen. Volgens Corstens doet het feit dat er slechts sprake is geweest van een globaal verzoek aan de betreffende burger om gegevens omtrent de criminele organisatie te verzamelen of dat de burger op eigen initiatief de gegevens heeft verzameld en verstrekt daar niets aan af.[184] Wij zijn het niet eens met dit standpunt. Het is immers denkbaar dat een informant gedurende een groot aantal jaren over veel verschillende personen praat, of slechts in hoofdlijnen bepaalde 'sfeerbeelden' verstrekt. Dat dit vanwege de duur van het contact zal leiden tot stelselmatigheid, is volgens ons moeilijk te verdedigen. Het gaat uiteindelijk om de informatie die de informant verstrekt omtrent een specifiek subject: op basis daarvan zal al dan niet sprake zijn van stelselmatigheid van de inbreuk op diens persoonlijke levenssfeer.

De discussie omtrent stelselmatigheid met betrekking tot het runnen van informanten laait weliswaar periodiek op, maar laat voorts onverlet dat de CIE-en in de praktijk nauwelijks gebruik maken van de mogelijkheden van artikel 126v WvSv: de basis voor het runnen blijft artikel 2 Politiewet 1993 en in de praktijk zijn CIE-

[184] Zie ook: Rechtbank Utrecht 18 april 2001, LJN AB1151. De rechtbank oordeelt dat uit de veelvuldige contacten tussen de runner en de informant moet worden afgeleid dat materieel kan worden gesproken van stelselmatige informatie-inwinning als bedoeld in artikel 126 WvSv. Er is ons echter geen andere jurisprudentie bekend waarin deze redenering van de rechtbank ook wordt gebruikt (zie Van der Bel et al. 2009: 151).

runners zeer terughoudend met een eventuele sturing. De informanten-informatie wordt dan ook, zoals we eerder hebben gezegd, slechts gebruikt als start- en sturingsinformatie en niet als bewijs. Volgens Kielman (2010: 47) leidt deze situatie tot het uitblijven van jurisprudentie omtrent de reikwijdte van artikel 126v WvSv. Hij stelt dat de in de praktijk gehanteerde definitie van stelselmatigheid op deze manier niet kan worden getoetst en het vermoeden rijst volgens hem dat een deel van de informanten ten onrechte op basis van artikel 2 Politiewet 1993 wordt gerund. Hier zijn wij het niet helemaal mee eens. De interpretatie van stelselmatigheid die in de praktijk wordt gehanteerd zal ook al moeten worden getoetst indien wordt gerund op basis van artikel 2 Politiewet 1993. Er rijzen immers pas problemen indien ten onrechte op basis van artikel 2 Politiewet 1993 wordt gerund met een meer dan lichte inbreuk op de privacy van het subject als gevolg. Uit de jurisprudentie volgt vooralsnog dat artikel 2 voldoende grondslag biedt. Het feit dat er zoveel verschillende zienswijzen mogelijk zijn, maakt het er voor de CIE in de praktijk overigens niet gemakkelijker op.

4.3.3 Een informant als verdachte

Het zou het gemakkelijkste zijn voor de CIE als zij spreekt met informanten die geen strafbare feiten plegen. Dit is echter niet mogelijk. De informanten waarmee de CIE spreekt, zijn vrijwel altijd betrokken (geweest) bij strafbare feiten. Het zijn immers met name mensen die zelf deel uitmaken van het criminele milieu en die derhalve daadwerkelijk over (goede) informatie omtrent strafbare feiten beschikken. Criminelen zijn zelf in dit opzicht dus de beste informanten. Dit kan echter ook tot problemen leiden, met name indien de informant wordt aangemerkt als verdachte.

Een CIE-informant kan op twee manieren voorkomen als verdachte. Hij kan (A) verdachte zijn van criminele activiteiten waarover hij geen informatie aan de CIE (heeft) verstrekt, of hij kan (B) zelf strafbare feiten plegen die in relatie staan tot de feiten waarover hij de CIE informeert en als zodanig aangemerkt worden als verdachte.

A: Verdachte van andere feiten

Allereerst behandelen wij de informant als verdachte van strafbare feiten waarover hij niet met de CIE spreekt. Een informant is een burger en het is hem dan ook in principe niet toegestaan strafbare feiten te plegen. Doet hij dit wel, dan kan hij als verdachte worden aangemerkt en kunnen opsporingsbevoegdheden tegen hem worden ingezet en kan hij worden vervolgd. Dit betekent echter niet dat hij niet meer als informant mag worden ingezet. De door hem gegeven informatie mag worden gebruikt en de CIE mag hem blijven runnen. In de praktijk zullen er echter belangrijke redenen zijn om dit niet te doen. Indien een informant verdachte is in een strafzaak en zijn telefoons worden getapt of hij wordt geobserveerd, dan is het erg moeilijk om met hem af te spreken en dit af te schermen van het tactische onderzoeksteam dat op hem werkt. Dit is echter een praktisch en geen juridisch beletsel (Van der Bel et al. 2009: 155-157). Het is wel tevens een juridisch beletsel indien de informant verdacht wordt van de feiten waarover hij verklaart.

B: Verdachte van feiten waarover de informant verklaart

Het is een informant niet toegestaan strafbare feiten te plegen die in relatie staan tot datgene waarover hij de CIE informeert (Van der Bel et al. 2009: 158). Zo mag hij bijvoorbeeld geen onderdeel uitmaken van de criminele organisatie waarover hij informatie verstrekt (artikel 140 Sr). De reden voor dit verbod is gelegen in de nasleep van de IRT-affaire: betrokkenheid van informanten bij de strafbare feiten waarover zij verklaren zal al snel het beeld oproepen van groei-informanten en de delta-methode. Met andere woorden: er is dan mogelijk sprake van burgerinfiltratie, en dit is, behoudens opsporingsonderzoeken naar terroristische misdrijven, uit den boze (zie subsectie 3.6.3; Van der Bel et al. 2009: 157 e.v.). De CIE wil zoveel mogelijk voorkomen dat informanten die op een bepaald moment verdacht worden van strafbare feiten aangeven dat ze deze feiten met medeweten van de CIE hebben gepleegd. Iedere informant krijgt voorafgaande aan diens inschrijving in het informantenbestand diverse spelregels te horen, waaronder de regel dat hij niet mag verklaren over strafbare feiten waarbij hij zelf betrokken is. Indien blijkt van strafbare betrokkenheid van de informant, dan zal het contact met de informant worden verbroken. In sommige gevallen is het denkbaar dat de informant door zijn runners wordt aangehouden, bijvoorbeeld indien hij een vuurwapen bij zich draagt (vanzelfsprekend wordt het vuurwapen in beslag genomen).

Vanwege het feit dat voorbereidingshandelingen (artikel 46 WvSr) ook strafbare feiten opleveren, kan er al snel sprake zijn van strafbare feiten van de kant van de informant. Dit maakt het runnen van informanten die actief zijn in de zware en georganiseerde criminaliteit erg lastig.[185] Vaak zullen slechts die informanten die tot een bepaalde kring van ingewijden van criminelen behoren, daadwerkelijk over goede informatie beschikken. Tot die kring geraken mensen doorgaans pas als ze zelf ook strafbare feiten plegen. Zoals een CIE-analist het tijdens een sociaal gesprek verwoordde: "*van de slager ga je het echt niet horen.*"

De strafbare feiten die een informant pleegt, komen voor zijn eigen rekening. Hij kan dus als verdachte worden aangemerkt en in die hoedanigheid in een opsporingsonderzoek voorkomen. Een verdachte kan zich nooit op zijn status als informant beroepen om bijvoorbeeld aan vervolging te ontkomen. Als een informant over strafbare feiten verklaart waarbij hij zelf betrokken is, mag de CIE de informatie niet gebruiken.

In uitzonderingsgevallen kan een informant met medeweten van de CIE en het OM wel strafbare feiten plegen die in relatie staan tot de feiten waarover hij de CIE informeert. Het gaat dan om pseudokoop of pseudodienstverlening, beide BOB-bevoegdheden (artikel 126ij tot 126z WvSv). Indien deze bevoegdheden worden ingezet, zal daarvan melding moeten worden gemaakt in het CIE-proces-verbaal. Dit maakt de afscherming van de informant erg moeilijk, en in de praktijk wordt er zelden van deze mogelijkheid gebruik gemaakt (Van der Bel et al. 2009: 158-160). Het is overigens in geen enkele situatie toegestaan dat de CIE-officier van justitie op eigen gezag opdracht geeft aan de informant om deel te nemen aan of samen te werken met de criminele organisatie waar de politie zich op richt. Dat zou namelijk burgerinfiltratie (artikel 126w WvSv) betekenen, waarvoor zeer strenge eisen gelden zoals toestemming van het College van Procureurs Generaal na vooraf overleg met de Minister van Veiligheid en Justitie (Van der Bel et al. 2009: 160). Alhoewel er een

[185] Op zichzelf is het feit dat informatie afkomstig is uit het criminele milieu naar het oordeel van de Hoge Raad irrelevant, zie HR 18 april 2000, LJN: ZD1771. Dit is dus nog geen reden om minder waarde aan de informatie te hechten.

juridische grondslag bestaat voor burgerinfiltratie, is dit toch uit den boze omdat er sprake is van een parlementair moratorium dat de toepassing van burgerinfiltratie (behoudens uitzonderingsgevallen) onmogelijk maakt (Corstens 2008: 468).

4.3.4 Runnen in de praktijk

We hebben hierboven de (juridische) theorie van het runnen van informanten behandeld. Maar hoe werkt het runnen in de praktijk? Om te kunnen runnen, moeten er informanten worden benaderd. Dit gaat op verschillende manieren. Vaak constateren runners of (indien de CIE daarover beschikt) analisten dat iemand een potentiële interessante informant kan zijn. Dit kan op basis van de ervaringskennis van de betreffende CIE-er, of op basis van de bevindingen uit een opsporingsonderzoek. Deze potentiële informant wordt dan, met toestemming van het hoofd CIE en de CIE-officier van justitie, benaderd. Deze benadering vindt bijvoorbeeld telefonisch plaats, of door middel van direct persoonlijk contact.

Runners onderhouden in koppels contact met de informanten, aan de ene kant om zoveel mogelijk de veiligheid van de runners te garanderen, aan de andere kant omdat twee vaak meer weten (en onthouden) dan één. De runners proberen een vertrouwensband met de informant op te bouwen. Dit vertrouwen is noodzakelijk om van de (meestal criminele) informant relevante informatie los te krijgen. Vaak duurt het een tijd voordat een potentiële informant de runners voldoende vertrouwt en daadwerkelijk openheid van zaken geeft (voor zover dat inderdaad gebeurt). Het gesprek begint doorgaans met het doornemen van de spelregels waaraan de informant zich dient te houden. De contacten vinden in beginsel in persoon plaats (dus niet telefonisch of per e-mail: deze communicatiemethoden worden slechts gebruikt bij de eerste benadering), meestal in openbare gelegenheden (zoals cafés) en niet zelden in de avonduren. In de ideale situatie voert de ene runner het gesprek en maakt de ander aantekeningen, maar in de praktijk wisselen ze ook wel eens van rol. Daarnaast zijn de mogelijkheden om aantekeningen te maken in de praktijk vaak beperkt: het valt al snel op wanneer drie mensen met elkaar spreken en één daarvan maakt gedurende het gehele gesprek aantekeningen. Een gesprek met een informant duurt gemiddeld een aantal uren. Een gemiddeld gespreksverslag bestaat uit twee of drie pagina's A-4 formaat. Wekelijks worden er tientallen informanten gesproken, hetgeen een behoorlijke hoeveelheid gespreksverslagen oplevert. Al met al is het runnen van informanten een tijdrovende bezigheid waar de CIE de handen vol aan heeft.[186]

4.3.5 Runnen exclusief door de CIE

Het runnen van informanten mag op basis van het derde lid van artikel 4 van de CIE-regeling uitsluitend worden verricht door de CIE. De keuze om het runnen van informanten (zowel op basis van artikel 2 Politiewet als artikel 126v WvSv) uitsluitend te laten uitvoeren door de CIE, wordt in de toelichting op de CIE-regeling als volgt toegelicht:[187] "*In de eerste plaats beschikt de criminele inlichtingen eenheid (voorheen als CID) over een jarenlange ervaring met het runnen van informanten. Daarmee is een grote mate van deskundigheid opgebouwd. In de tweede plaats schuilt in het organisatorisch onderscheid maken tussen het runnen van 'tactische' informanten en het runnen van de overige informanten het gevaar van inconsistent*

[186] De informatie uit deze subsectie is afkomstig van diverse medewerkers van de CIE die wij tijdens ons veldwerk hebben gesproken.
[187] Stcr. 2000, 12 oktober 2000, nr. 198, p. 14.

beleid en gebrek aan overzicht, hetgeen uiterst ongewenst is. Bovendien vergemakkelijkt concentratie van de runnerstaak een uniforme wijze van informantgegevens."

Het is andere onderdelen van de politie dus niet toegestaan om informanten te runnen. Het runnen van informanten is voorbehouden aan de CIE en is in de praktijk de primaire wijze van informatieverzameling door de CIE. De vraag die nu rijst is of de CIE ook andere opsporingsbevoegdheden kan inzetten om informatie te verzamelen.

Of de inzet van BOB-middelen ook betekent dat de daarmee verzamelde informatie tot het bewijs dient te worden gerekend, is binnen de CIE-wereld een onderwerp van discussie. Volgens de CIE-officieren volgt niet uit de wetsgeschiedenis van de wet BOB dat informatie die is verzameld door middel van de inzet van BOB-middelen niet gebruikt kan worden als start- en sturingsinformatie ('intelligence' volgens deze officieren). De Memorie van Toelichting maakt volgens de officieren nergens onderscheid tussen de toepassing van bijzondere opsporingsbevoegdheden voor het verkrijgen van bewijs of voor het verkrijgen van start- en sturingsinformatie (Van der Bel et al. 2009: 142). De officieren zijn dus van mening dat de bevoegdheden van de wet BOB ook ten behoeve van het verzamelen van start- en sturingsinformatie kunnen worden ingezet en gaan er dus van uit dat in de CIE-fase (de proactieve voorfase waarin er nog geen sprake is van een tactisch opsporingsonderzoek) bepaalde BOB-middelen kunnen worden ingezet ten behoeve van de CIE-taak.

Wij sluiten ons grotendeels aan bij de lezing van de officieren, maar merken hierbij wel het volgende op. De belangrijke vraag in dit opzicht is met welk doel de informatie wordt verzameld. Is het doel het verzamelen van start- en sturingsinformatie, dus informatie op basis waarvan strafvorderlijke beslissingen kunnen worden genomen? Of gaat het om het verzamelen van informatie met als doel het verkrijgen van een informatiepositie? Indien wordt geaccepteerd dat ook de CIE-fase valt onder de definitie van opsporing, dan is het inzetten van BOB-middelen met als doel het verzamelen van start- en sturingsinformatie toegestaan. Niet toegestaan is het inzetten van BOB-bevoegdheden louter ten behoeve van de opbouw en instandhouding van de informatiepositie. Hierin verschilt de CIE van de AIVD: de AIVD heeft juist de opbouw en instandhouding van een informatiepositie als zelfstandige doelstelling. Uiteindelijk moet het doel van de inzet van opsporingsbevoegdheden zijn het vervolgen en berechten van verdachten.

4.4 Verwerken

Als informatie is verzameld, dan wordt het door de CIE opgeslagen in gegevensbestanden. Dit is de tweede fase van het CIE-proces: de verwerking. Omdat de WPG het belangrijkste juridische kader is voor de verwerking van CIE-gegevens, staan wij in subsectie 4.4.1 kort stil bij deze wet. De verwerking van politiegegevens afkomstig van informanten betreft alle waarnemingen, afspraken en bevindingen in relatie tot de informant, de persoon van de informant en de verstrekte informatie. Een dergelijke gegevensverwerking is in de eerste plaats noodzakelijk zodat de runners zich een beeld kunnen vormen van de achtergronden en gedragingen van de informant en van de met hem in een eerder stadium gemaakte afspraken. Deze zogenoemde 'artikel 12 verwerkingen' (genoemd naar het relevante artikel uit de WPG) behandelen wij in subsectie 4.4.2. Daarnaast dient deze gegevensverwerking als basis voor verdere gegevensverwerking door de CIE. Het betreft hier de zogenaamde bruto-

informatie die aanleiding kan vormen tot de terbeschikkingstelling van gegevens binnen de CIE met het oog op verdere veredeling van die gegevens.[188] Hierbij wordt gedoeld op het proces waarbij de uit de bruto-gespreksverslagen gedestilleerde netto-informatie (beide vallende binnen het artikel 12-domein) middels een speciaal formulier ('4x3tje' in CIE-jargon) kunnen worden opgeslagen in het zogenoemde zwacri-domein (artikel 10 lid 1 sub a WPG). Deze laatste verwerkingen komen in subsectie 4.4.3 aan bod

4.4.1 De Wet Politiegegevens als juridische grondslag

Wij hebben in de voorgaande subsecties al een paar keer gerefereerd aan de WPG. De op 1 januari 2008 ingevoerde Wet politiegegevens[189] (WPG) reguleert de verwerking van gegevens door de politie, en daarmee dus ook de gegevensverwerking door de CIE. Voor een meer volledige behandeling van deze wet verwijzen wij naar Van der Bel et al. (2009) en Koelewijn (2009). Wij zullen hier slechts de verwerking van politiegegevens kort behandelen.

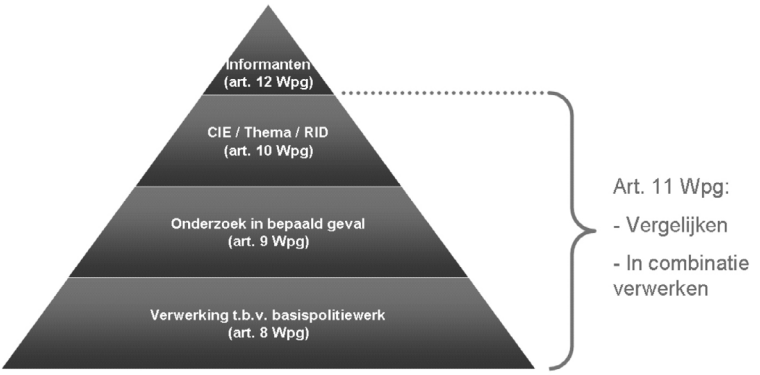
De WPG ziet op de verwerking van politiegegevens. De vraag is evenwel: wanneer is er sprake van een politiegegeven? En wanneer van een verwerking? Artikel 1 sub a WPG geeft de definitie van 'politiegegeven': elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon dat in het kader van de uitoefening van de politietaak wordt verwerkt. In de praktijk zijn alle gegevens die de CIE verzamelt in het kader van de CIE-taak politiegegevens. Onder 'verwerken van politiegegevens' wordt ingevolge artikel 1 sub c WPG verstaan: elke handeling of geheel van handelingen met betrekking tot politiegegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, vergelijken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van politiegegevens. Er zal in vrijwel alle gevallen waarin er iets met politiegegevens wordt gedaan, sprake zijn van een verwerking. Dit betekent dat nagenoeg alle handelingen die betrekking hebben op politiegegevens onder het regime van de WPG vallen. De WPG stelt in artikel 3 verder dat de verwerking van politiegegevens slechts kan plaatsvinden voor welomschreven en gerechtvaardigde doelen en voor zover de verwerking van gegevens evenredig is aan het betreffende doel.[190] Maar voor welke doeleinden kunnen politiegegevens worden verwerkt?

De WPG kent vier soorten verwerkingen, ieder met een eigen doel. De eerste is de verwerking ten behoeve van de uitvoering van de dagelijkse politietaak (artikel 8 WPG). Het gaat hierbij bijvoorbeeld om informatie die tijdens een surveillance door een straatagent wordt verzameld. De tweede soort is de verwerking ten behoeve van een onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval (artikel 9 WPG). Dit zijn bijvoorbeeld de tactische opsporingsonderzoeken. De derde soort betreft de verwerking ten behoeve van: (1) de CIE-taak (inzicht in de zware en georganiseerde criminaliteit, artikel 10 lid 1 sub a WPG), (2) de themaverwerkingen (mensenhandel, mensensmokkel en terrorisme, artikel 10 lid 1 sub b WPG) of (3) de RID-taak (artikel 10 lid 1 sub c). De vierde soort verwerking in het kader van de

[188] *Kamerstukken II*, 2005-06, 30 327, nr. 3, p. 56.
[189] Wet van 21 juli 2007, houdende regels inzake de verwerking van politiegegevens (Wet politiegegevens), Stb. 2007, 300.
[190] *Kamerstukken II*, 2005-06, 30 327, nr. 3, p. 3.

WPG is de verwerking van politiegegevens ten behoeve van het beheer van informanten (artikel 12 WPG). Deze verwerking kent speciale waarborgen vanwege de afscherming van de identiteit van de informant. Naast de hier genoemde vier zelfstandige grondslagen voor het verwerken van politiegegevens kent de WPG ook nog een mogelijkheid tot het vergelijken (op basis van *hit /no hit*) en het onder bepaalde voorwaarden in combinatie verwerken van politiegegevens uit de artikelen 8, 9 en 10 WPG wanneer een verwerking op basis van artikel 9 of 10 WPG daartoe aanleiding geeft (artikel 11 WPG). Artikel 11 WPG biedt dus geen zelfstandige basis voor gegevensverwerking, maar verruimt de mogelijkheden van artikel 9 en 10 verwerkingen. Voor de toepassing van de gecombineerde verwerking van artikel 11 lid 4 WPG gelden enkele zware procedurele eisen. Zo is er een opdracht van het bevoegd gezag vereist en kan de verwerking slechts plaatsvinden bij zeer ernstige inbreuken op de rechtsorde.

In figuur 4.1 zijn de vier soorten verwerkingen opgenomen, waarbij geldt dat hoe hoger de verwerking in de piramide zit, des te meer restricties er gelden voor die verwerking. Deze restricties worden aangebracht door middel van autorisaties. Voor de verwerkingen die hoger in de piramide staan, worden minder mensen geautoriseerd dan voor de verwerkingen lager in de piramide. Deze gelaagde opbouw heeft te maken met de bescherming van de privacy van de betrokken personen van wie gegevens worden verwerkt. Daarnaast is deze gelaagde opbouw bedoeld om het afbreukrisico zo veel mogelijk te beperken: hoe minder politiemensen bij de meest gevoelige informatie kunnen, des te kleiner de kans dat deze informatie 'weglekt'.



Figuur 4.1: De grondslag voor WPG-verwerkingen

Zoals de structuur van de WPG aangeeft, neemt de CIE bij het verwerken van politiegegevens een bijzondere positie in: zij bevindt zich boven in de piramide. Voor dit onderzoek zijn dan ook de verwerking van politiegegevens op basis van artikel 10 en 12 relevant. In de subsectie 4.4.2 behandelen wij de artikel 12-verwerkingen. Subsectie 4.4.3 ziet op de artikel 10 lid 1 sub a WPG verwerking.

4.4.2 Artikel 12-verwerkingen

De CIE verwerkt een gesprek in een zogenoemd bruto-gespreksverslag ('de bruto' in CIE-jargon). Dit wordt vervolgens opgeslagen in een zogenaamd 'informantengegevensbestand'. De juridische grondslag voor deze verwerking is

artikel 12 WPG. Artikel 12 WPG biedt geen grondslag voor andere verwerkingen dan verwerkingen die zijn gericht op het beheren van informanten. Het verslag is een woordelijke weergave van het gesprek tussen de runner en de informant. Hier staan ook mededelingen van persoonlijke aard van de informant aan de runner en de wijze waarop de runners het contact hebben ervaren. De bruto bevat dus zowel strafrechtelijk relevante informatie als informatie die niet strafrechtelijk relevant is. Deze laatste informatie wordt toch opgenomen in een verslag omdat het kan helpen om een beeld te krijgen van de informant en van het verloop van de gesprekken. Wij bespreken in deze subsectie verder nog (A) de autorisaties voor artikel 12 informatie en (B) de veredeling van de in het kader van artikel 12 verwerkte gegevens.

(*A) Autorisaties artikel 12-informatie*

Voor de artikel 12-verwerkingen kunnen allereerst de runners die contact onderhouden met de informant worden geautoriseerd. Daarnaast is het hoofd van de CIE en diens plaatsvervanger geautoriseerd, alsmede de CIE-officier van justitie. In bepaalde gevallen zijn ook CIE-analisten geautoriseerd voor het verwerken van deze informatie. De belangrijkste regel is echter dat alleen medewerkers van de CIE geautoriseerd mogen worden voor artikel 12-verwerkingen. De toegang tot artikel 12-politiegegevens is dus voorbehouden aan medewerkers die werkzaam zijn bij de CIE en die deze politiegegevens ook daadwerkelijk nodig hebben voor hun werkzaamheden.[191] De wetgever hangt de autorisaties aan functionaliteit en niet aan rang. Dit betekent dat mensen die in het lijnmanagement een hogere positie hebben, zoals leden van de korpsleiding, niet op basis van hun rang automatisch voor de politiegegevens die in het kader van artikel 12 WPG worden verwerkt worden geautoriseerd.

(*B) Veredeling*

Informatie afkomstig van informanten is per definitie subjectieve informatie: het gaat immers om informatie uit tweede of derde hand. Voordat er met deze informatie verder kan worden gewerkt, zal zij waar mogelijk moeten worden veredeld. Dit betekent dat de informatie wordt beoordeeld op juistheid en nauwkeurigheid. Kielman (2010: 41) spreekt overigens van volledigheid als eis in plaats van nauwkeurigheid. Wij houden ons echter aan de terminologie die de wetgever hanteert. Nauwkeurigheid en volledigheid zijn immers verschillende eisen.

Een runner veredelt informatie op verschillende wijzen. Wij noemen er drie. Allereerst gebruikt een runner zijn intuïtie (zie ook Kielman 2010: 41-42). De runner gebruikt bij deze vorm van veredeling zijn kennis en ervaring om de bron en de informatie te beoordelen. Is het logisch wat de informant vertelt, of zijn er redenen om aan de informatie of informant te twijfelen? Dit is een vrij 'zachte' manier van veredelen, maar desalniettemin vindt het in de praktijk veelvuldig plaats. De tweede wijze van veredeling is het vergelijken van de informatie met informatie uit andere bronnen. Zo kunnen door de informant verstrekte personalia worden vergeleken met de GBA of bedrijfsgegevens met het Kadaster. Informatie die door deze bronnen wordt bevestigd, zal vrij snel als betrouwbaar kunnen worden aangemerkt. Het is ook de praktijk dat runners de andere politiebestanden bevragen om informatie te veredelen. Voor zover zij dit doen ten behoeve van het beheren van de informant

[191] Artikel 2:3 lid 5 Bpolg.

biedt artikel 12 WPG hiervoor de grondslag. Op basis van dit artikel kan echter enkel naar bevestigende of ontkrachtende informatie worden gezocht. Het is niet de bedoeling dat de runner (of in bepaalde gevallen een analist) informatie aan het verslag toevoegt, bijvoorbeeld iets dat de informant zelf niet heeft gezegd. Dit is een onderdeel van de analysetaak waarvoor artikel 10 lid 1 sub a WPG de juridische grondslag biedt en voorwaarden stelt (zie subsectie 4.5.3). De derde wijze van veredeling komt voort uit de historische relatie met de informant. Is de informant in het verleden veelal betrouwbaar geweest, kwam hij de afspraken na? Overigens moet in dit opzicht een onderscheid worden gemaakt tussen de betrouwbaarheid van de informatie en de betrouwbaarheid van de informant. De informant kan volledig te goeder trouw onjuiste informatie verstrekken. Indien dit laatste vaker gebeurt, zullen er bij de veredeling vraagtekens bij de informatie worden gezet. In sectie 4.6 gaan we hier nader op in.

4.4.3 Zwacri-verwerkingen van artikel 10 lid 1 sub a WPG

Het uiteindelijke doel van de CIE is niet het beheren van de informant, maar het ter beschikking stellen van strafrechtelijk relevante informatie aan een opsporingsteam (of andere belanghebbende) (zie ook de in subsectie 4.2.2 beschreven taakstelling). Hiertoe dient de CIE over een informatiepositie te beschikken. Zij dient inzicht te hebben in de wereld van de zware en georganiseerde criminaliteit. Artikel 10 lid 1 sub a WPG spreekt in dit opzicht van 'het verkrijgen van inzicht in de betrokkenheid van personen bij de zware- en georganiseerde criminaliteit'. Dit worden ook wel 'zwacri-verwerkingen' of de 'inzichttaak van de CIE' genoemd. De inzichttaak is de analyse van de informatie afkomstig van informanten. De in het zwacri-domein opgeslagen gegevens worden met name door de CIE geanalyseerd met de volgende doelen:

(1) het signaleren van criminaliteitsontwikkelingen;

(2) het periodiek verslag doen ten behoeve van criminaliteitsbeelden;

(3) het verrijken van geregistreerde informatie, wat kan leiden tot gegevens die zich direct lenen voor operationeel gebruik.

Kort gezegd ziet de analysetaak op het verwerken van zwacri-informatie ten behoeve van inzicht. De CIE-regeling schrijft echter niet dwingend voor dat deze analysetaak enkel binnen de CIE kan worden belegd. Het is denkbaar (en inmiddels ook praktijk) dat andere eenheden binnen de politie worden belast met het (een deel van) de analysetaak. De CIE heeft zoals gezegd (subsectie 4.2.4) weinig analisten in dienst die deze inzichttaak kunnen uitvoeren. In de praktijk ligt de nadruk van het CIE-werk dan ook met name op het verzamelen van informatie door middel van het runnen van informanten. De analyse die binnen de organisatorische eenheid van de CIE plaatsvindt, is doorgaans beperkt tot de analyse van verzamelde inlichtingen en is direct ondersteunend aan de inwintaak. De algemene analysetaak wordt doorgaans door de RIO's vervuld. Dit neemt echter niet weg dat het hoofd CIE verantwoordelijk blijft voor deze algemene analysetaak.

In tegenstelling tot de handelingen bij het veredelen van informatie, wordt in de inzichtfase de informatie gecombineerd en geïnterpreteerd.[192] Met andere woorden: informatie wordt omgezet in kennis. Zo wordt de strafrechtelijk relevante informatie gecombineerd met informatie uit andere bronnen, zoals opsporingsonderzoeken of open bronnen. Verder proberen de analisten en rechercheurs een beeld te krijgen van wat de georganiseerde criminaliteit is en wie daarbij betrokken zijn. In principe wordt er in deze fase geen gebruik gemaakt van bijzondere opsporingsbevoegdheden, maar gaat het echt om het analyseren van informatie die al binnen de politie aanwezig is of vrij beschikbaar is in het openbare (publieke) domein. De informatie die al binnen de politie aanwezig is, is afkomstig uit lopende en afgesloten opsporingsonderzoeken of afkomstig van informanten en kent daarom doorgaans een hoog afbreukrisico. De autorisaties tot deze artikel 10-gegevens zijn daarom vaak beperkt tot een afgebakende groep politiemedewerkers.

De autorisaties voor artikel 10-gegevens worden nader uitgewerkt in artikel 2:5 lid 1 Bpolg. De toelichting op dit artikel stelt allereerst dat, gelet op de belangen van de bescherming van de persoonlijke levenssfeer en de tactische afscherming, moet worden voorkomen dat de betreffende gegevens binnen de politie beschikbaar zijn buiten een kleine kring van politieambtenaren die betrokken zijn bij de gegevensverwerking.[193] Voor autorisaties zouden in de eerste plaats in aanmerking kunnen komen politieambtenaren die werkzaam zijn bij de CIE van het betreffende korps. Daarnaast zullen *in voorkomende gevallen* ook andere ambtenaren van politie, zoals medewerkers van de infodesk of misdaadanalisten, moeten kunnen worden geautoriseerd voor de verwerking van CIE-gegevens. De kring van te autoriseren personen zal echter beperkt moeten zijn tot de politieambtenaren die taken of werkzaamheden verrichten op het gebied van de CIE. Het feit dat artikel 2:5 spreekt van 'in voorkomende gevallen' geeft onzes inziens aan dat het hier een uitzondering op de hoofdregel betreft. De hoofdregel is dat slechts medewerkers die werkzaam zijn bij de CIE kunnen worden geautoriseerd tot de gegevens die worden verwerkt op grond van artikel 10 lid 1 sub a WPG.

De toedeling van autorisaties aan niet bij de CIE werkzame politieambtenaren dient na overleg en in overeenstemming met het hoofd van de CIE plaats te vinden. Deze autorisaties kunnen slechts worden toebedeeld wanneer dit dringend noodzakelijk is voor een goede uitvoering van de politietaak.

Uit artikel 2:6 Bpolg volgt voorts dat het OM dient in te stemmen met beleidsafspraken over de te autoriseren categorieën van politieambtenaren die kunnen worden belast met bepaalde gegevensverwerkingen. Vanuit het oogpunt van de strafrechtelijke handhaving van de rechtsorde gaat het om gegevensverwerkingen met een bijzonder risico. Het betreft met name de gegevensverwerking over de informanten, de themaverwerking en de CIE-verwerking.[194] De autorisatie voor het zwacri-domein betekent overigens niet per definitie dat de betreffende medewerker toegang heeft tot alle politiegegevens binnen dat domein. Ook binnen het 'zwacri-domein' kunnen verschillende autorisaties worden toegekend.

Hoewel mensen uit andere organisatieonderdelen kunnen worden geautoriseerd voor CIE-gegevens, betekent dit niet dat deze CIE-gegevens buiten het CIE-domein vallen en daarmee buiten de verantwoordelijkheid van het hoofd CIE.

[192] Wij wijzen er op dat in bepaalde gevallen er een gecombineerde verwerking plaatsvindt, waardoor artikel 10 lid 1 sub a WPG niet langer de grondslag voor de verwerking biedt, maar het striktere regime van artikel 11 lid 4 WPG van toepassing is.
[193] Nota van Toelichting bij Bpolg, *Stb.* 2007, 550, p. 38.
[194] *Ibid.*, p. 39.

Het hoofd CIE (of zijn plaatsvervanger) is in artikel 2:10 lid 2 Bpolg aangewezen als 'bevoegd functionaris'. De bevoegd functionaris moet instemmen met verdere verwerking van politiegegevens voor een ander doel dan artikel 10 lid 1 sub a WPG.[195] Dit betekent dat wanneer men politiegegevens vanuit artikel 10 wil gebruiken voor bijvoorbeeld een tactisch onderzoek of het delen van politiegegevens met 'blauwe diensten' (de politieafdelingen die zijn belast met de surveillance en noodhulpverlening), het hoofd CIE hiermee moet instemmen. Hieruit vloeit voort dat het hoofd CIE politiegegevens voorziet van een codering ter indicatie van de vertrouwelijkheid van die gegevens (11, 01, 00, 200 en 300, zie subsectie 4.5.1).

De bevoegd functionaris dient ook zijn instemming te geven aan de verdere verwerking van gegevens na het geautomatiseerd vergelijken van politiegegevens op basis van artikel 11 lid 2 WPG en het in combinatie verwerken van politiegegevens op basis van artikel 11 lid 4 WPG. Autorisaties aan andere medewerkers dan CIE-medewerkers dienen te worden vastgesteld in overeenstemming met het hoofd CIE.[196]

In veel regiokorpsen is de CIE organisatorisch ondergebracht bij een RIO. De medewerkers van de RIO worden belast met het analyseren van (zware) criminaliteit, en verrichten daarmee hun werkzaamheden op basis van artikel 10 lid 1 sub a WPG. Deze werkzaamheden vallen dan ook onder de verantwoordelijkheid van het hoofd CIE. Dit houdt in dat het hoofd CIE juridisch gezien zeggenschap heeft over de politiegegevens die verwerkt worden in de RIO's. Immers, verantwoordelijkheid zonder bevoegdheid is moeilijk denkbaar. In de praktijk is men nog nauwelijks doordrongen van deze consequentie van de WPG. Het hoofd CIE heeft helemaal geen zeggenschap over de RIO en de informatieproducten die door de RIO worden opgeleverd, en wordt bijvoorbeeld niet om toestemming gevraagd voor de relevante autorisaties (behoudens de autorisatie tot de informanten informatie: de 11, 01, 00, 200 en 300 informatie). Het is interessant om te bezien hoe de politie hiermee in de toekomst omgaat. Wij sluiten deze sectie af met de vaststelling dat volgens onze definitie van de CIE (definitie zeven, sectie 1.2) de RIO als CIE kan worden aangemerkt. Zij voert immers een deel van de CIE-taak uit.

4.4.4 Terrorisme: themaverwerking

De wetgever heeft bepaald dat voor bepaalde categorieën misdrijven de opbouw en instandhouding van een permanente informatiepositie onontbeerlijk is. Dit zijn de zogenoemde 'themaverwerkingen' van artikel 10 lid 1 sub b WPG. De volgende drie thema's worden in artikel 2:3 Bpolg (limitatief) benoemd: terrorisme, mensenhandel en mensensmokkel. Deze themaverwerkingen bieden de politie de mogelijkheid om ook gegevens te verwerken over groepen van onverdachte personen ten aanzien waarvan aanknopingspunten bestaan dat zij betrokken kunnen zijn bij handelingen die wijzen op het beramen, voorbereiden of plegen van misdrijven die verband houden met het thema.

De themaverwerkingen worden geregeld in artikel 10 lid 1 sub b WPG. De overeenkomst met de zwacri-verwerking is dat de themaverwerkingen ook zien op het opbouwen van een informatiepositie. Deze mogelijkheid is bij een themaverwerking zelfs nog ruimer dan bij de zwacri-verwerking, omdat ook gegevens mogen worden verwerkt van mensen tegen wie aanwijzingen bestaan dat zij in een bepaalde relatie staan tot de drie genoemde thema's (bij de verwerkingen in het kader van de CIE-taak

[195] Ingevolge artikel 10 lid 5 WPG.
[196] Nota van Toelichting bij Bpolg, *Stb.* 2007, 550, p. 39.

moet er sprake zijn van een verdenking. Dit is een zwaardere eis dan de aanwijzingen uit de themaverwerking). Dit maakt het mogelijk om over een grotere categorie van mensen informatie te verwerken. De themaverwerkingen zijn voor dit onderzoek bijzonder relevant, omdat de wetgever in de toelichting aangeeft dat de opbouw en instandhouding van een informatiepositie bij de genoemde thema's onontbeerlijk is.[197] Dat komt omdat van de politie op die thema's wordt verwacht dat zij zich met name richt op het voorkomen van de strafbare feiten die tot het thema kunnen worden gerekend. Deze preventieve taak vereist een proactieve werkwijze, hetgeen dicht bij de taak en werkwijze van de AIVD ligt. In hoofdstuk zeven meer over de themaverwerkingen en de manier waarop ze in de praktijk een rol (kunnen) spelen bij IGP.

4.5 Verstrekken

Het laatste onderdeel van het CIE-proces is het verstrekken van politiegegevens. Voordat wij inhoudelijk op dit onderwerp ingaan, maken wij eerst een opmerking over de gehanteerde terminologie. De term 'verstrekking' wordt in de WPG gebruikt voor verstrekkingen door de politie aan individuen of instanties die niet tot de politie behoren, het gaat dus om de externe verstrekkingen. De wet spreekt wanneer het gaat om interne verstrekkingen om het 'ter beschikking stellen van politiegegevens'. Wij hanteren echter in beide gevallen de term verstrekking omdat dit onzes inziens duidelijker is.

Onder 'verstrekken van politiegegevens' verstaat de WPG het bekend maken of ter beschikking stellen van politiegegevens, ongeacht de wijze waarop dit gebeurt (mondeling, schriftelijk of langs elektronische weg, artikel 1 sub c WPG). Ook als een persoon over de schouder van een ander meekijkt, dan geldt dit als een verstrekking. Dus het laten zien van een (powerpoint-) presentatie met daarin informatie over subjecten, geldt tevens als een verstrekking in de zin van de WPG. Onder 'ter beschikking stellen' verstaat de WPG 'het verstrekken van politiegegevens aan personen die overeenkomstig de WPG zijn geautoriseerd voor het verwerken van politiegegevens'.

Bij verstrekkingen van politiegegevens door de CIE geldt bronbescherming als absolute voorwaarde. Vanwege deze bronbescherming wordt de CIE vaak als 'sectie stiekem' aangeduid: CIE-ers zullen namelijk nooit informatie aan anderen verstrekken die de identiteit van een informant bekend maakt buiten een zeer kleine groep die deel uitmaakt van de CIE. Deze afscherming van de identiteit is overigens geen absoluut recht: de toegezegde afscherming kan vervallen als zich zwaarwegende belangen voordoen, bijvoorbeeld indien er sprake is van een op handen zijnde aanslag op het leven van derden (Van der Bel et al. 2009: 202). Behoudens deze uitzonderingen is het uitgangspunt dat de CIE geen informatie verstrekt die de identiteit van de informant bloot kan leggen. De CIE werkt echter niet in een isolement. Zij maakt deel uit van de politieorganisatie in algemene zin en verzamelt informatie ten behoeve van die bredere politieorganisatie. Kortom, de CIE zal wel informatie moeten verstrekken aan de overige onderdelen van de politieorganisatie. In subsectie 4.5.1 behandelen wij de verstrekkingen van politiegegeven die worden verwerkt op basis van artikel 12 WPG (het artikel 12-domein). Vervolgens behandelen we in subsectie 4.5.2 de verstrekkingen van de in het kader van artikel 10 verwerkte politiegegevens (het artikel 10-domein).

[197] *Kamerstukken II*, 2005-06, 30 327, nr. 3, p. 48.

4.5.1 Verstrekking uit artikel 12-domein

Politiegegevens uit het informantenbestand van artikel 12 WPG kunnen gedurende een periode van maximaal vier maanden ter beschikking worden gesteld voor verdere verwerking in het kader van (1) de dagelijkse politietaak (artikel 8 WPG), (2) een concreet onderzoek (artikel 9 WPG) of (3) het verkrijgen van inzicht in de betrokkenheid van personen bij de zware georganiseerde criminaliteit (artikel 10 WPG). Het verstrekken van informatie uit het artikel-12 domein naar onderzoeken binnen het artikel 10 domein (zwacri) is een zwaarwegend punt van aandacht. Het betekent immers dat politiegegevens uit het informantenregister worden verstrekt aan politieambtenaren die geautoriseerd zijn voor de zwacri-verwerking (artikel 10 lid 1 sub a WPG). Technisch gezien betekent dit dat de gegevens in een 'andere bak' worden geplaatst en de gegevens juridisch gezien anders worden geclassificeerd, namelijk: geschikt voor de zwacri-verwerking (zie hieronder het 4*3-formulier). Er zitten ook politiegegevens in het informantenregister die nooit voor een andere verwerking dan de informantenverwerking (artikel 12 WPG) in aanmerking komen. Het gaat dan om de identificerende gegevens van de informant en de bruto-gespreksverslagen. Deze informatie is voorbehouden aan de CIE.

Bij de behandeling van verstrekkingen van artikel 12-gegevens, kunnen de volgende drie onderwerpen niet ontbreken: (A) het 4*3 formulier dat voor verstrekkingen wordt gebruikt, (B) de beoordeling van de betrouwbaarheid van de informant en (C) de gehanteerde verstrekkingscoderingen.

*A: 4*3 formulier*

Informatie uit het artikel 12-domein wordt naar het artikel 10-domein overgebracht door middel van een speciaal formulier. Dit formulier heet het criminele inlichtingenrapport (CIR, in een enkele regio ook wel 'Zwacri Informatie Rapport' oftewel 'ZIR' genoemd). De in de praktijk meer gebruikte naam is het 4*3 formulier (4*3-tje in CIE-jargon). Deze formulieren mogen alleen worden gebruikt binnen het CIE-domein, dus voor verstrekking van informatie binnen de eigen CIE of tussen CIE-en onderling (Van der Bel et al. 2009: 169).

B: Controle informant

In het 4*3 formulier geeft de CIE een oordeel omtrent de betrouwbaarheid van de informant. De informant wordt beoordeeld op (1) de betrouwbaarheid van de informatie, (2) de controleerbaarheid en (3) de zakelijke relatie tussen de informant en diens runners. Hiervoor worden codes gehanteerd. Code A betekent dat de informant betrouwbaar is en zich aan de gemaakte afspraken houdt. Code B houdt in dat de informant meestal betrouwbaar is en zich meestal aan de gemaakte afspraken houdt. Code C geeft aan dat de informant niet betrouwbaar is en zich in het verleden niet aan de werkafspraken heeft gehouden. In deze gevallen wordt de informatie over het algemeen niet verstrekt. Het is immers onvoorstelbaar dat de CIE informatie verstrekt waarvan zij weet dat deze onjuist is. De laatste code is X, en dit betekent dat de informant niet te beoordelen is. Vaak gaat het om informanten waar de CIE nog niet zo lang contact mee heeft.

Naast de beoordeling van de betrouwbaarheid geeft de CIE door middel van andere codes ook inzicht in de wijze waarop de informatie door de informant is verkregen. Code 1 betekent dat de informant het zelf heeft waargenomen: hij was bij

de feiten aanwezig waarover hij verklaarde. Code 2 geeft aan dat hij het van iemand heeft gehoord die de feiten waarover hij verklaart zelf heeft waargenomen. Code 3 betekent dat de informant het via via heeft. Het zal duidelijk zijn dat informatie met code 3 erg zachte informatie is. Een informant met code A 1 is dus een betrouwbare informant die de feiten waarover hij heeft verklaard zelf heeft waargenomen.

Deze codes (A,B,C,X en 1, 2, 3) geven gecombineerd deels inzicht in de mogelijke betrouwbaarheid van de informatie voor zover de CIE dat kon beoordelen. Het is namelijk altijd mogelijk dat een informant in het verleden betrouwbaar is gebleken en dus een A of B code krijgt, maar liegt over een door hem gedane waarneming en daar onterecht een 1 scoort. Daarnaast kan hij complete leugens vertellen zonder dat de CIE daar achter komt. Bovendien is de CIE beperkt in haar middelen om dit te controleren. Dat is een belangrijk verschil met de AIVD. De CIE heeft doorgaans namelijk niet de capaciteit om BOB-middelen in te zetten om de informanten te controleren. Voorts zijn de CIE-en terughoudend omdat het risico bestaat dat de CIE constateert dat informanten zelf ook bij het beramen of plegen van strafbare feiten betrokken zijn (dezelfde of andere strafbare feiten dan waarover zij verklaren), en hiervan zal dan proces-verbaal moeten worden opgemaakt met als mogelijk gevolg dat de betreffende informant de focus wordt van een opsporingsonderzoek. De al dan niet terechte angst bestaat dat het informantenbestand zo wel erg snel wordt uitgedund. En ook voor de bronafscherming is deze situatie onwenselijk. Immers, in het kader van een opsporingsonderzoek kan blijken dat een verdachte door de CIE wordt gerund, bijvoorbeeld omdat de runners over de tap komen. Een AIVD heeft in dit opzicht meer mogelijkheden, al gaat het dan niet om BOB-middelen maar om bijzondere inlichtingenmiddelen. Naast de hierboven genoemde veredeling is een andere belangrijke manier waarop een CIE een informant gericht kan controleren het zoeken van andere informanten in diens omgeving die over dezelfde feiten wat kunnen vertellen. Op deze manier kunnen informanten kruislings worden beoordeeld. In de praktijk is dit zeer omslachtig en niet altijd mogelijk. Binnen de CIE-en wordt er dan ook soms voor gepleit om BOB-bevoegdheden toe te laten ter controle van de informanten, dit gecombineerd met een belangrijke rol van een rechter-commissaris bij het beoordelen van de rechtmatigheid van werken door de CIE (zie voor de rol van een rechter-commissaris Brinkhoff 2009: 125 e.v.).

C: Verstrekkingscodering: 00, 01, 11, 200 en 300 informatie

De CIE geeft in het 4*3 rapport ook een code die aangeeft op welke wijze de informatie uit het rapport kan worden gebruikt door de ontvanger (over het algemeen is de ontvanger een andere CIE). Deze codes kennen een enigszins aparte nummering. Zo wordt code 11 gehanteerd voor informatie die tactisch te gebruiken is. Deze informatie wordt uit verschillende bronnen bevestigd en is dus niet herleidbaar tot een concrete informant. Code 01 wordt gebruikt voor informatie die in principe wel tactisch te gebruiken is, maar waarvoor eerst toestemming nodig is van het hoofd van de CIE waar de informatie is binnengekomen. Indien informatie code 00 krijgt (‘dubbel-0’ in CIE-jargon), dan is de informatie niet tactisch te gebruiken omdat het inzicht zou kunnen geven in wie de informant is. Als er slechts twee personen op de hoogte zijn van een bepaald strafbaar feit (en dat van elkaar weten), en één daarvan is informant en verklaart over dat feit, dan is het voor de ander al vrij snel duidelijk van wie die informatie afkomstig is. Deze informatie krijgt dus de code 00.

Informatie met code 200 kent een verhoogd afbreukrisico met betrekking tot de inhoud van de informatie. Indien de informatie bekend zou worden, geeft dat niet zozeer aan wie de informant is, maar geeft het wel inzicht in bijvoorbeeld lopende onderzoeken. Deze code wordt vaak gegeven aan informatie met betrekking tot corruptie: indien deze informatie tactisch wordt gebruikt, is de kans groot dat een eventueel onderzoek bekend wordt bij de verdachte. De laatste code die de CIE hanteert, is code 300. Deze informatie kent een verhoogd risico voor de afscherming van de informant. Codes 200 en 300 worden doorgaans gebruikt voor bijzonder gevoelige informatie. Over het algemeen volstaat men binnen de CIE met codering 11, 01 en 00.

Als de informatie door middel van een 4*3 formulier aan het artikel 10-domein is verstrekt, bevindt de informatie zich nog steeds in dit 'CIE-domein'. In de volgende subsectie behandelen wij de verstrekking vanuit deze zwacri-omgeving naar het artikel 9 WPG domein.

4.5.2 Verstrekking uit het artikel 10-domein

Politiegegevens uit de zwacri-omgeving (artikel 10 lid 1 sub a WPG) kunnen, met instemming van een daartoe bevoegd functionaris, ter beschikking worden gesteld voor verdere verwerking in het kader van de dagelijkse politietaak, een concreet onderzoek of het informantenbestand. Ingevolge artikel 2:10 lid 2 Bpolg wordt met 'bevoegd functionaris' bedoeld het hoofd van de betreffende CIE of diens plaatsvervanger.[198] Voor dit onderzoek zijn verder twee zaken van belang: (A) verstrekkingen door de CIE buiten het CIE-domein geschieden door middel van een CIE-PV en (B) verstrekkingen van 'bijvangst' verdient speciale aandacht; bijvangst wil zeggen informatie die niet afkomstig is van informanten en daarom ook minder afscherming behoeft.

A: CIE-PV

Indien informatie door de CIE wordt verstrekt aan een tactisch opsporingsteam, dan wordt er van een speciaal CIE proces-verbaal gebruik gemaakt. Een verstrekking van CIE-informatie buiten de CIE vindt slechts plaats door het hoofd van de CIE of diens plaatsvervanger. Zij zijn de opsporingsambtenaren die bevoegd zijn om een CIE proces-verbaal op de stellen en te ondertekenen: runners en analisten mogen formeel juridisch niet zelfstandig verstrekken.

Er is geen wettelijke regeling die verstrekking door middel van proces-verbaal verplicht stelt, maar het behoort binnen de CIE-wereld tot de gangbare praktijk waarvan doorgaans niet wordt afgeweken (zie ook: Van der Bel et al. 2009: 176). Een proces-verbaal wordt aan het onderzoeksdossier toegevoegd, wat maakt dat de officier van justitie altijd op de hoogte is van wat de CIE aan het tactische opsporingsteam heeft verstrekt. De officier is immers eindverantwoordelijke en dient de activiteiten die in het kader van een onderzoek hebben plaatsgevonden voor de rechter te verantwoorden. Dit zou erg lastig worden indien de verstrekte CIE-informatie anders dan door middel van proces-verbaal wordt verstrekt.

[198] De tekst van de bepaling biedt overigens ruimte om meerdere personen aan te wijzen die als vervanger van het hoofd CIE instemming kunnen verlenen.

Het is in uitzonderingsgevallen overigens wel mogelijk om CIE-informatie mondeling aan een tactisch opsporingsteam te verstrekken. Indien uit CIE-informatie gevaar blijkt voor de veiligheid van anderen en het gaat om een actueel gevaar, dan mag er eerst mondeling worden verstrekt. Achteraf zal de mondelinge verstrekking wel altijd door een proces-verbaal worden gevolgd. Indien er bij de CIE informatie binnenkomt waaruit blijkt dat een verdachte vuurwapengevaarlijk is en een aanhouding ophanden is, dan kan het zijn dat de CIE dit mondeling aan de tactisch teamleider mededeelt. De aanhouding geschiedt dan door middel van de inzet van een Arrestatie-Team (AT).

Dezelfde CIE-informatie mag meerdere keren middels een proces-verbaal worden verstrekt, er is geen rechtsregel die zich daartegen verzet (zie Van der Bel et al. 2009: 181). Om dubbeltelling van informatie te voorkomen, dienen de verschillende teamleiders wel op de hoogte te worden gesteld van het feit dat de informatie ook aan een ander team is verstrekt. Indien dit niet gebeurt, dan kan het lijken alsof de informatie uit verschillende bronnen afkomstig is, terwijl er feitelijk slechts één informant is.

B: Bijvangst

Het komt voor dat de CIE-runners informatie krijgen die niet voldoet aan de criteria voor opname in de artikel 10 lid 1 sub a bestanden. Dit wordt 'bijvangst' genoemd. Deze bijvangst kan ook worden verstrekt door middel van een proces-verbaal. Runners beschikken overigens naast hun specifieke taak in het kader van de CIE-regeling ook over de algemene opsporingsbevoegdheden waar iedere opsporingsambtenaar over beschikt. Indien zij kennis krijgen van strafbare feiten die niet voldoen aan de zwacri-criteria, dan mogen zij deze informatie op basis van artikel 2 Politiewet 1993 opslaan en verstrekken. Overigens worden deze gegevens wel opgenomen in een artikel 12-bestand: ze kunnen immers inzicht geven in de informant.

Naast de bijvangst is het ook denkbaar dat een runner zelf relevante feiten constateert. Hij ziet op weg naar huis bijvoorbeeld een ontmoeting tussen hem bekende subjecten. Ook deze informatie kan worden verstrekt. Zoals gezegd is de runner een opsporingsambtenaar, dus is hij bevoegd om een proces-verbaal van bevindingen op te maken. Overigens kan de CIE van alle relevante niet-informanten informatie een dergelijk proces-verbaal van bevindingen opmaken. Dit geldt ook voor de zogenoemde 'rest- en zijtakinformatie' (informatie uit lopende of afgesloten onderzoeken die niet voor dat concrete onderzoek relevant zijn, maar wel voor andere opsporingsonderzoeken). Ook anonieme tips of informatie uit open bronnen wordt door middel van een proces-verbaal van bevindingen verstrekt.

4.5.3 Verstrekkingen aan de AIVD

Naast de bovengenoemde verstrekkingen zijn in het kader van dit onderzoek met name de verstrekkingen aan de AIVD van belang. Politieambtenaren (dus ook runners van de CIE) kunnen tijdens het werk in aanraking komen met informatie die van belang kan zijn voor de AIVD. De wijze van verstrekking aan de AIVD verschilt van de hierboven beschreven wijze van verstrekking aan andere onderdelen van de politie. De WIV 2002 voorziet voor deze gevallen in een verstrekkingbepaling. Artikelen 61 en 62 WIV 2002 verplichten onder meer de ambtenaren van de politie om te beoordelen of informatie relevant kan zijn voor de dienst, en zo ja, deze te

verstrekken.[199] Het gaat hier om een verplichting. Dit is overigens een belangrijke aanwijzing voor de aard van de verhouding tussen de politie en de AIVD: de dienst heeft de discretionaire bevoegdheid informatie aan de politie te verstrekken (zie subsectie 3.4.2), terwijl de politie een verplichting heeft. Hieruit volgt in ieder geval dat de wetgever een bepaalde hiërarchie heeft aangebracht tussen de organisaties, waarbij de bescherming van de nationale veiligheid van groter belang wordt geacht dan de bestrijding van criminaliteit (zie ook subsectie 8.4.2).

Artikelen 60 en 61 leggen weliswaar een verplichting op om te verstrekken, ze voorzien echter niet in een tijdsbepaling. De politie heeft dus ruimte om te bepalen wanneer ze de informatie verstrekt. Daarnaast is het aan de politie om te beoordelen of de informatie binnen de taakomschrijving van de dienst valt: hier zou zij met creatieve interpretatie wellicht nog ruimte hebben om gegevens achter te houden.[200] Aan de formele hiërarchie moet dus niet teveel gewicht worden toegekend.

In het arrest van de Hoge Raad van 28 maart 2003, NJ 2004, 71 wordt daarnaast een ruimte voor een belangenafweging aan het OM toegekend. Volgens de Hoge Raad moeten de verplichtingen van art. 61 WIV 2002 niet blindelings worden nageleefd, zonder rekening te houden met onder meer de bescherming van de veiligheid van personen en andere zwaarwegende belangen. Zo kan het OM volledige en absolute geheimhouding garanderen aan de informant om zo bepaalde belangrijke informatie van die informant te verkrijgen, en het belang om op deze manier informatie te krijgen kan zwaarder wegen dan het belang van de dienst om de informatie te verkrijgen (Van der Bel et al. 2009: 286-289).[201] De verplichting van artikel 61 WIV 2002 is daarmee niet absoluut, en het ligt voor de hand dat deze ruimte ook geldt voor artikel 62 (de politie), waarbij wij opmerken dat dit slechts opgaat voor zover het OM dit goedkeurt.[202] De hierboven beschreven ruimte van de politie met betrekking tot classificatie en tijdstip van verstrekking is volgens de wetgever kennelijk ongewenst: in de WPG probeert hij hier een einde aan te maken. Artikel 24 WPG stelt namelijk dat de politie een geautomatiseerde vergelijking van de eigen gegevens met die van de dienst dient mogelijk te maken. De AIVD kan op basis van een zogenoemd *hit/no hit* systeem de politiesystemen bevragen op de aanwezigheid van voor de taakuitoefening van de AIVD relevante gegevens. Indien

[199] Een dergelijke relevantie wordt geacht aanwezig te zijn indien de informatie past binnen de taakstelling van de AIVD. Artikel 61 regelt de verplichting van het OM, artikel 62 de verplichting van de politie. Formeel dient de verstrekking van deze gegevens door de politie eerst aan een 'artikel 60-ambtenaar' plaats te vinden.

[200] Informatie met betrekking tot terrorisme valt overigens altijd onder de taak van de AIVD: het is immers moeilijk vol te houden dat terrorismebestrijding niet tot de taak van de AIVD behoort. Bij terrorismebestrijding geldt dus met name de ruimte van de politie om zelf te bepalen wanneer ze de gegevens verstrekt. Overigens merken wij ook op dat het hier om mogelijkheden gaat die de wet biedt. Of deze ruimte in de praktijk ook daadwerkelijk wordt gebruikt, is ons niet bekend.

[201] De runners garanderen de informant dat zijn identiteit alleen bij het hoofd CIE en de CIE officier van justitie bekend wordt. Het is dan moeilijk aan de informanten uit te leggen dat er ook nog een andere organisatie de identiteit krijgt, en dat je niet weet hoeveel mensen dan uiteindelijk van de identiteit van informanten op de hoogte zijn. De bereidheid van informanten om informatie te verstrekken zal waarschijnlijk afnemen indien teveel mensen achter de identiteit komen.

[202] De Hoge Raad geeft immers het OM de bevoegdheid om een belangenafweging te maken en een volledige en absolute geheimhouding te garanderen. Omdat het OM en de politie over dezelfde informatie beschikken zou het echter vreemd zijn als het OM een belangenafweging maakt waarbij hij tot de conclusie komt dat verstrekking aan de AIVD niet plaats dient te vinden, maar de politie exact dezelfde gegevens wel moet verstrekken aan de AIVD. Het ging in het betreffende arrest overigens over toezeggingen die zijn gedaan aan een informant. Informanteninformatie is de meest gevoelige categorie van politie-informatie, en het is dus zeker niet gezegd dat met betrekking tot andere categorieën van politie-informatie ook ruimte is voor het afwegen van verschillende belangen.

de politie inderdaad zulke gegevens heeft, krijgt de dienst een hit en dient de politie de overeenkomende gegevens en de achterliggende gegevens direct geautomatiseerd aan de dienst te verstrekken. Dit wetsartikel biedt de politie dus veel minder ruimte voor eigen afwegingen (zie sectie 8.9 voor hoe dit artikel in de praktijk lijkt te werken).

Bij verstrekkingen van informatie aan de AIVD geldt het zogenoemde 'geen actie zonder overleg' (GAZO) principe (Van der Bel et al. 2009: 288). Dit betekent dat de AIVD geen gebruik zal maken van de CIE-informatie zonder dat hierover overleg is geweest. Het betekent echter niet dat er overleg met de CIE plaatsvindt. Indien de CIE informatie aan de AIVD verstrekt, dan doet zij dit allereerst door tussenkomst van de CIE-officier van justitie. Daarna gaat de informatie naar de landelijke officier van justitie belast met terrorismebestrijding. Deze officier van justitie beoordeelt of de informatie inderdaad van belang is voor de AIVD voor het vervullen van zijn taak.

4.6 Hoofdstukconclusie

Deze laatste sectie plaatst de bevindingen uit dit hoofdstuk in het licht van de LP-kenmerken zoals beschreven in hoofdstuk twee. Deze kenmerken zijn (A) handhaving van de rechtsorde, (B) waarheidsvinding, (C) het opsporingsonderzoek als werkproces en (D) transparantie in het kader van het strafrecht. In deze laatste sectie behandelen wij in hoeverre deze kenmerken gelden voor de CIE en beantwoorden wij OV1 specifiek voor de CIE.

A: Handhaving van de rechtsorde (LP-kenmerk 1)

De CIE heeft als taak de informatievoorziening in het kader van de uitvoering van de politietaak met betrekking tot zware en georganiseerde criminaliteit en terrorisme. Hieruit volgt in algemene zin dat de CIE als onderdeel van de politie belast is met de handhaving van de rechtsorde (dit is namelijk een onderdeel van de politietaak zoals geformuleerd in artikel 2 Politiewet 1993). Zij doet dit weliswaar in de informationele voorfase, maar desalniettemin is de CIE een onderdeel van de politie en richt zij zich op de handhaving van de rechtsorde. Voorts volgt uit de genoemde specifieke taakstelling van de CIE in de CIE-regeling dat de CIE slechts informatie mag inwinnen over de zware (georganiseerde) criminaliteit en terrorisme. Het is een CIE niet toegestaan om structureel over 'lichtere' vormen van criminaliteit informatie te verzamelen en zeker niet om informatie te verzamelen over onderwerpen die niet in relatie staan tot de zware (en georganiseerde) criminaliteit en/of terroristische misdrijven. De CIE is dus belast met het handhaven van het deel van de rechtsorde waarop de zware (georganiseerde) criminaliteit en terrorisme een inbreuk maken.

Met dit kenmerk doelen we ook op het gegeven dat de politie in algemene zin slechts in situaties handhavend kan optreden indien er sprake is van een van tevoren door de wetgever strafbaar gestelde handeling of gedraging. Handelingen of gedragingen die niet van tevoren strafbaar zijn gesteld, vallen niet onder de rechtsorde en de politie kan hier niet handhavend optreden (behoudens de handhaving van de openbare orde, maar dat valt buiten het bereik van dit onderzoek). Net als de andere onderdelen van de politie is het de CIE niet toegestaan om informatie te verzamelen over handelingen en gedragingen die buiten het bereik van de rechtsorde vallen en dus niet strafbaar zijn. Het eerste kenmerk (de handhaving van de rechtsorde) is dus ook van toepassing op de CIE.

B: Waarheidsvinding (LP-kenmerk 2)

De handhaving van de rechtsorde door de politie vindt plaats door waarheidsvinding. Wij beschouwen de waarheidsvinding in het opsporingsonderzoek eenvoudigweg als het onderzoek verricht door de politie naar wat er feitelijk is gebeurd met betrekking tot één of meer vermoedelijk begane strafbare feiten. De politie probeert de materiële waarheid vast te stellen aan de hand van bewijs. Zij construeert hiertoe allereerst een verhaal omtrent hetgeen is gebeurd, en aan de hand van concreet bewijs wordt dit verhaal al dan niet bevestigd. De politie is daarmee per definitie een reactieve organisatie die zich primair richt op het verleden. Dit geldt in hoofdlijnen ook voor de CIE.

Door middel van het runnen van informanten verzamelt de CIE informatie over zware en georganiseerde criminaliteit en terrorisme. Dit wordt in de praktijk gezien als de hoofdtaak van de CIE. Dat maakt dat ook de CIE primair reactief werkt in de zin dat de CIE de tactische opsporingsteams ondersteunt bij het vaststellen van wat er in een bepaald geval precies is gebeurd. De juridische taak van de CIE is echter breder dan enkel het runnen van informanten ten behoeve van de materiële waarheidsvinding.

Op basis van artikel 4 van de CIE-regeling en artikel 10 lid 1 sub a WPG is de CIE ook belast met het verkrijgen van inzicht in zware en georganiseerde criminaliteit en terrorisme. Deze inzichttaak wordt door de wetgever ook wel 'de CIE-taak' genoemd, en deze taak is in hoofdregel bij de CIE neergelegd. Een onderdeel van de CIE-taak is dus het zicht krijgen op ontwikkelingen in de zware en georganiseerde criminaliteit. Deze toekomstgerichte taak van de CIE lijkt op de voorwaarschuwingsfunctie van de AIVD. In dit opzicht vertoont de CIE met betrekking tot dit tweede kenmerk in juridisch opzicht gelijkenis met zowel de AIVD als de politieorganisatie in het algemeen. Wij hebben echter ook vastgesteld dat de nadruk in de praktijk voornamelijk ligt op het verzamelen en verstrekken van informatie, en niet zozeer op het analyseren van de verzamelde informatie. De CIE mist analysecapaciteit om aan deze analysetaak in de praktijk een goede uitvoering te kunnen geven. Wij stellen daarom vast dat het tweede kenmerk van de politie, te weten waarheidsvinding door middel van reactieve activiteiten, in grote mate ook voor de CIE geldt.

C: Het opsporingsonderzoek als werkproces (LP-kenmerk 3)

De waarheidsvinding vindt plaats door middel van een opsporingsonderzoek. De CIE heeft een bijzondere positie in het Nederlandse opsporingsonderzoek. Formeel worden de opsporingsonderzoeken verricht door de tactische opsporingsteams en is de CIE ondersteunend. De CIE-informatie wordt om redenen van afscherming van de identiteit van de informant vaak buiten het tactische opsporingsproces gehouden. Deze afscherming heeft binnen de politie weliswaar tot gevolg dat de CIE is afgescheiden van de rest van de rechercheorganisatie, maar dit neemt niet weg dat de CIE een onderdeel is van de rechercheorganisatie van de politie. Het CIE-proces maakt dus deel uit van het opsporingsproces: door de CIE verstrekte processen-verbaal worden in het procesdossier opgenomen, CIE-chefs en CIE-runners kunnen worden opgeroepen om te compareren *et cetera*. Een CIE-runner is daarnaast net als de tactische rechercheurs een opsporingsambtenaar die gebonden is aan de regels die gelden voor de opsporing. Indien door het optreden van de CIE een stelselmatige

inbreuk op de persoonlijke levenssfeer van een persoon wordt gemaakt, dan moet daarvoor een strafvorderlijke bevoegdheid zijn (artikel 126v of 126zt WvSv).

Er zijn echter twee belangrijke verschillen met de tactische opsporing. Het eerste verschil is dat de CIE als hoofdregel geen bewijs verzamelt. De CIE werkt (naar eigen zeggen) met intelligence: informatie die slechts gebruikt kan worden als start- en sturingsinformatie en niet als bewijs in strafvorderlijke zin. Het tweede verschil met de tactische opsporingsteams is dat de CIE het enige onderdeel van de politie is dat informanten mag runnen. En het runnen van informanten is dus traditioneel één van de manieren waarop de politie informatie over zware criminaliteit verzamelt. Deze informatie heeft echter wel een strafvorderlijke kwalificatie (start- en sturingsinformatie) en valt daarmee onder het opsporingsproces.

Net als de overige opsporing, wordt het werkproces van de CIE in verregaande mate gereguleerd. Dit werkproces valt uiteen in de volgende drie fasen: (a) verzamelen, (b) verwerken en (c) verstrekken van inlichtingen. Met betrekking tot het verzamelen van informatie stellen wij vast dat de CIE dit primair doet door middel van het runnen van informanten en in mindere mate door het verzamelen van rest- en zijtak informatie uit lopende onderzoeken of informatie uit open bronnen. Met name de mate van sturing van een informant is een belangrijk juridisch en praktisch vraagstuk waar de CIE mee te maken heeft. Dat zij zo min mogelijk de informant sturen, is een belangrijk verschil met de AIVD. Een groot deel van de overige regelgeving met betrekking tot de verwerking en verstrekking van gegevens ziet op de afscherming van de identiteit van de informant bij de verwerking en verstrekking van CIE-gegevens.

Wij stellen dan ook vast dat alhoewel de CIE is gescheiden van de tactische opsporingsteams, zij toch een onderdeel is van het bredere opsporingsproces, zij het een bijzonder onderdeel. Dit brengt ons tot het vierde en laatste traditionele kenmerk van de politie in het algemeen: transparantie.

D: Transparantie in het kader van het strafrecht (LP-kenmerk 4)

Zoals wij hebben hoofdstuk twee hebben gesteld, is één van de belangrijkste uitgangspunten van het strafrecht dat het optreden van politie en justitie transparant is. Zowel de strafrechter als de verdediging dienen in de positie te zijn om het verhaal van politie en justitie te toetsen. De hoofdregel van de politie dient dus transparantie te zijn. Dit geldt echter niet voor de CIE. De CIE schermt veel van haar informatie af om de identiteit van informanten te beschermen. Zo stelt de CIE-regeling eisen aan de fysieke afscherming van de CIE en zijn de autorisaties voor CIE-informatie beperkt tot een kleine groep medewerkers van de politie die in hoofdregel werkzaam zijn bij de CIE. In dit opzicht is de CIE niet transparant. Dit is dan ook de reden dat de CIE-informatie niet wordt aangemerkt als bewijs, maar als start- of sturingsinformatie. Het is overigens aan de strafrechter om te beoordelen of hij de CIE-informatie al dan niet rekent tot het bewijs, en de strafrechter kan ook openheid van de CIE eisen, zelfs daar waar het de identiteit van informanten betreft. De geheimhouding binnen de CIE is dus niet absoluut. Dit is een belangrijk verschil met de AIVD, waar geheimhouding in beginsel wel absoluut is. Omdat wij onderzoek verrichten naar de verhouding tussen de AIVD en de CIE, merken wij hier op dat het in deze context niet zozeer van belang is in hoeverre er objectief gezien sprake is van transparantie. Het gaat er met name om in hoeverre er volgens de AIVD sprake is van transparantie. Het feit dat CIE-informatie, alhoewel bewerkt, wordt opgenomen in een procesdossier en het uiteindelijk aan de strafrechter is om te bepalen in hoeverre de CIE openheid van

zaken moet geven, zal de AIVD weinig gerust stemmen. Informatie-uitwisseling met de CIE zal ook een zeker risico met zich meebrengen. Ook voor de CIE geldt dus dat er sprake is van de 'tirannieke werking van het procesdossier', zij het in mindere mate dan bij de tactische opsporingsteams. De hoofdregel van de CIE is en blijft echter geheimhouding. Dit geldt zelfs voor verstrekkingen aan de AIVD. In hoeverre er objectief sprake is van geheimhouding is overigens wel van belang bij het andere onderdeel van ons onderzoek: de implementatie van IGP. De geheimhouding bij de CIE staat haaks op één van de uitgangspunten van IGP, te weten *need to share*. Dit is het onderwerp van hoofdstuk vijf. Met betrekking tot het vierde onderwerp (de relatie met de context) stellen wij echter vast dat de CIE in het algemeen niet gekenmerkt wordt door transparantie, maar door geheimhouding.

Wanneer we alle kenmerken van de traditionele politie vergelijken met de kenmerken van de CIE, dan zien we al vrij snel dat de CIE veel kenmerken van de traditionele politie heeft. In het volgende hoofdstuk zullen we bezien wat IGP is en hoe dit concept zich verhoudt tot de hier behandelde kenmerken van de traditionele politie.

5| De intelligencegestuurde politie

Dit hoofdstuk beantwoordt OV 2: *Wat is het concept IGP en hoe beoogt dit concept de traditionele Nederlandse CIE te veranderen?* Wij schetsen in dit hoofdstuk primair wat de politiediensten met IGP beogen, en gaan nog niet in op de praktijk van IGP. Deze praktijk is het onderwerp van hoofdstuk zeven.

De term intelligencegestuurde politie (IGP) duikt voor het eerst op in Engeland in het begin van de jaren '90 van de vorige eeuw. Het wordt daar '*intelligence led policing*' (ILP) genoemd. In Kent ontwikkelde de plaatselijke politie een sturingsconcept waarin de politie haar activiteiten coördineert op basis van geanalyseerde misdaadinformatie: ILP (zie Gill 2000: Ratcliffe 2008). Door informatie omtrent autodiefstal en andere criminaliteit te combineren en te analyseren, bleek het lokale politiekorps in staat om verdachten te identificeren die betrokken waren bij veel criminele feiten. Zo kon de politie gericht het criminaliteitsprobleem aanpakken. In het vervolg gebruiken wij de Nederlandse naam voor *intelligence led policing*, intelligencegestuurde politie (IGP). IGP is tegenwoordig een veel breder concept dan aan het begin van de jaren '90. Bovendien is het inmiddels verworden tot een wereldwijd concept dat het politiewerk dient te hervormen.

Wij geven in dit hoofdstuk de relevante achtergronden van IGP en behandelen een aantal implicaties voor de politiepraktijk. Dit doen wij aan de hand van relevante literatuur. De resultaten van ons eigen empirische onderzoek naar de praktijk van IGP staan in hoofdstuk acht.

Wij beginnen in sectie 5.1 met een korte beschrijving van de historische ontwikkeling van IGP aan de hand van diens voorlopers, *community policing* en de probleemgestuurde politie. In sectie 5.2 behandelen wij vervolgens de nieuwe ontwikkelingen die een belangrijke invloed op IGP hebben. Sectie 5.3 ziet op de theoretische verklaring voor het ontstaan en de werking van IGP. In sectie 5.4 gaan wij dieper in op het concept van IGP. Wat wenst de politie nu eigenlijk met IGP te bewerkstelligen? Wij doen dit met name aan de hand van het begrip 'intelligence'. Sectie 5.5 beziet IGP in Nederland. In sectie 5.6 vergelijken wij het concept IGP en de Nederlandse uitwerking daarvan met de door ons in hoofdstuk 2 geformuleerde kenmerken van politieke intelligence. Wij introduceren nieuwe begrippen en geven een andere analyse van IGP dan doorgaans gebruikelijk is. In sectie 5.7 geven wij een antwoord op OV 2 en sluiten wij af met algemene hoofdstukconclusies.

5.1 Historische ontwikkelingen

In de laatste jaren zijn er grote veranderingen geweest, zowel voor de politiediensten in Europa als in de Verenigde Staten. Reorganisaties, structurele veranderingen en voortdurende heroriëntering op de werkwijze en doelstellingen waren aan de orde van de dag. Met het oog op de ontwikkelingen van IGP is het einde nog niet in zicht. Natuurlijk, de politie is altijd al op zoek geweest naar nieuwe concepten die de dienst structureel zouden kunnen verbeteren. Ieder concept dient daarbij specifieke belangen en zet andere belangen weer op de achtergrond. Zo zijn '*community policing*' en 'de probleemgestuurde politie' binnen de politieorganisatie al jaren lang gevleugelde termen. Deze concepten zijn als het ware de voorlopers van IGP. IGP draagt elementen van beide concepten in zich. We zullen daarom beginnen met *community*

policing (subsectie 5.1.1). Daarna behandelen wij de probleemgestuurde politie (subsectie 5.1.2).

5.1.1 Community policing

De jaren '60 en '70 van de vorige eeuw zijn politiek en sociaal-maatschappelijk roerige jaren geweest. De V.S. waren het toneel van rassenrellen en wereldwijd was er veel verzet tegen de oorlog in Vietnam en tegen het kapitalisme in het algemeen. *Community policing* wordt in deze periode met name in de V.S. in het politiewerk geïntroduceerd (Hahn 1998: 71-74; Van der Torre en van Harmelen 2007: 920-924). Het is een directe reactie op de onrusten van de jaren '60 en de geconstateerde breuk tussen de samenleving en de overheid, de politie daarbij inbegrepen (Eck en Spellman 2005: 412-414). De politie moest dichter bij de samenleving komen te staan en weer een onderdeel van de maatschappij worden.

Ook in Nederland werd het concept *community policing* snel opgepakt en ingevoerd (zie Fijnaut 2006: 863 e.v.). Vanaf 1977 kreeg *community policing* een centrale rol in het Nederlandse politiebestel. De projectmatige invoering van het gebiedsgebonden politiewerk werd aan de Projectgroep Organisatiestructuren (POS) overgelaten (Van der Torre en Van Harmelen 2007: 918-919). In Nederland is het concept bekend geworden onder de naam 'gebiedsgebonden politiewerk', een variant van 'wijkgebonden politiezorg'. De inmiddels vertrouwde wijkagent is een onderdeel van de Nederlandse invulling van *community policing* (Van der Vijver en Terpstra 2007: 359).[203] De Nederlandse benadering van dit concept wijkt op hoofdlijnen echter af van de Angelsaksische benadering.

In tegenstelling tot de VS en Groot-Brittannië, werd in Nederland de discretionaire bevoegdheid van de wijkagenten niet aan banden gelegd, maar juist gekoesterd (Van der Torre 1999: 25). Daar waar de Amerikanen en Britten een toegenomen verantwoordingsplicht als een onlosmakelijk onderdeel van *community policing* zagen en dus uitgingen van de bestaande hiërarchische verhoudingen, leek de Nederlandse politie juist te kiezen voor een organisatorische verandering die de politie meer vrijheden moest geven. Vanaf de jaren '80 streefde men er in Nederland naar om de hiërarchisch georganiseerde politieorganisatie waar tot dan toe sprake van was om te vormen tot een postbureaucratische politieorganisatie, met onder meer gedeconcentreerde wijkteams (Van der Torre 1999: 27; zie ook Fijnaut 2006: 871 e.v.). Het komt er kort gezegd op neer dat hiërarchische zeggenschap over de politieagent in Nederland wordt losgelaten; de lagere politieambtenaar krijgt meer vrijheid en discretionaire bevoegdheden.

Community policing heeft een grote invloed gehad op IGP. Er zijn dan ook drie elementen van *community policing* die terugkomen in IGP. Dit zijn (1) de nadruk op proactiviteit, (2) het stimuleren van samenwerking met andere instanties en de bevolking in het algemeen en (3) het streven naar een vergroting van de effectiviteit van het politieoptreden (zie ook sectie 5.4).

Community policing en IGP verschillen echter in twee opzichten van elkaar. Allereerst is er binnen *community policing* een grote discretionaire ruimte van de politieambtenaar. Dit wordt binnen IGP gezien als een belemmering van een effectieve en efficiënte sturing van de Nederlandse politie en is iets dat veranderd

[203] Zij beschrijven overigens dat in de jaren '80 de oude, bekende wijkagent in teamverband moest gaan werken en zich meer op 'het echte politiewerk' moest richten. De klacht over de wijkagent was namelijk dat hij de grote problemen onaangeroerd liet of te gemakkelijk wetsovertredingen door de vingers zag (zie Van der Vijver en Terpstra 2007: 359).

dient te worden om IGP daadwerkelijk mogelijk te maken. Een tweede aspect waarin *community policing* afwijkt van IGP is de problematiek waar het zich op richt. Omdat problemen vanuit de samenleving worden aangedragen, betekende *community policing* in de praktijk dat politiemensen relatief veel tijd kwijt waren aan kleine criminaliteit en overlast waar de buurtbewoners last van hebben. Van criminaliteitsbestrijding in de zin van 'boeven-vangen' is bij *community policing* nauwelijks sprake.

Een concept dat in Nederland nooit echt voeten aan de grond heeft gekregen maar desalniettemin een bijzonder grote invloed op IGP heeft gehad, is de probleemgestuurde politie.

5.1.2 De probleemgestuurde politie

De probleemgestuurde politie werd in 1981 in de Verenigde Staten geïntroduceerd en vrijwel direct overgenomen in Groot-Brittannië (Scott 2000: 13). Diverse politiediensten implementeerden het concept en sindsdien wordt het breed toegepast. De probleemgestuurde politie kreeg ook in Nederland toepassing, zei het minder dan in de V.S. of Groot-Brittannië. Het doel van de probleemgestuurde politie is, kort gezegd, de politie effectiever te maken. Het streven van de politie moet niet slechts het verbeteren van de huidige politiepraktijk zijn, maar men moet zoeken naar de beste oplossing voor een specifiek probleem (Goldstein 1979; Scott 2000: 5). Het gehele politiewerk wordt onder de loep genomen en nauwkeurig onderzocht om op basis van de bevindingen een effectieve(re) strategische aanpak van bepaalde problemen te formuleren (Goldstein 1979: 405; 2003: 7). Problemen moeten effectief worden beïnvloed door bijvoorbeeld de schade te beperken of het probleem geheel dan wel gedeeltelijk op te lossen. De politie realiseert dit door zich met name te richten op de oorzaken die aan de problemen ten grondslag liggen.

De probleemgestuurde politie heeft een aantal kenmerken. Wij noemen de drie belangrijkste. Het eerste kenmerk is het uitgangspunt van de probleemgestuurde politie: de politie moet zoveel mogelijk problemen voorkomen; er moet met name naar preventieve maatregelen worden gekeken (Scott 2000: 7). Preventie van problemen speelt dus ook in dit concept al een belangrijke rol. Als preventie niet lukt, dan is een proactieve aanpak de beste methode. De nadruk op preventie en proactiviteit is voorts een belangrijk element van IGP (zie ook subsectie 5.4.2).

Het tweede belangrijke kenmerk is dat de oplossingen voor problemen niet alleen in het politieapparaat worden gezocht, maar ook daarbuiten. In dit opzicht is de probleemgestuurde aanpak een fundamentele afwijking van andere pogingen om het politiewerk effectiever te maken. Oplossingen worden over het algemeen gezocht bij de politieorganisatie zelf. Zij nemen bijvoorbeeld de vorm aan van meer bevoegdheden en voorgestelde wetswijzigingen (zie Scott 2000: 7). De actieve participatie van anderen dan de politie bij het oplossen van de problemen is een essentieel verschil met het bovenstaande *community policing*, waar de samenleving 'slechts' hielp bij het identificeren en prioriteren van problemen die de politie vervolgens moest behandelen. Overigens moeten deze verschillen tussen politieconcepten niet worden overtrokken: vaak worden *community policing* en de probleemgestuurde politie namelijk in één adem genoemd (zie ook Ratcliffe 2008: 70). IGP heeft beide benaderingen in zich: de buitenwereld is van belang, maar wordt met name gezien als een grote bron van informatie. Prioriteiten worden binnen IGP door de politie zelf gesteld, waarbij een grote nadruk ligt op criminaliteitsbestrijding.

Het derde kenmerk is een nauwkeurige probleemanalyse (Tilley 2003: 2; Ratcliffe 2008: 71). De probleemgestuurde politie richt zich op de analyse van verzamelde data om patronen te identificeren en daarmee tot een mogelijke oplossing van het probleem te komen. Dit vereist een lange termijn aanpak, iets waar veel politiediensten weinig ervaring mee hadden. Bij de probleemgestuurde politie spelen informatie en analyse een belangrijke rol (Scott 2000: 8-9; Tilley 2003: 4).

In tegenstelling tot *community policing* is de methode van de probleemgestuurde aanpak in Nederland niet echt invloedrijk geweest. Toch heeft ze wel een aantal sporen achtergelaten. Zo is de integrale aanpak van criminaliteit, waarbij de politie samenwerkt met maatschappelijke belangengroepen en partners om specifieke problemen op te lossen, een voorbeeld van een (gedeeltelijke) toepassing van de probleemgestuurde politie. Het idee dat de politie niet de enige verantwoordelijke is voor het veiligheidsvraagstuk, wordt in dit concept geformuleerd.

5.2 Nieuwe ontwikkelingen

Net als bij haar voorgangers komt IGP voort uit bepaalde sociaal maatschappelijke ontwikkelingen. Het is een reactie op bredere ontwikkelingen in de maatschappij. Wij kunnen in dit hoofdstuk niet alle ontwikkelingen beschrijven die een invloed hebben gehad op de politie en beperken ons tot vijf, te weten (1) een noodzaak tot effectiever en efficiënter politiewerk (subsectie 5.2.1), (2) de opkomst van de georganiseerde criminaliteit (subsectie 5.2.2), (3) de opkomst van terrorisme (subsectie 5.2.3), (4) de schaalvergroting van het politiewerk (subsectie 5.2.4) en (5) de ontwikkeling naar een risicosamenleving (subsectie 5.2.5).

5.2.1 Effectiviteit en efficiency

IGP is volgens de 'politielegende' ontstaan in Kent, Groot-Brittannië in de voor de Engelse politie turbulente jaren '80 en '90 van de vorige eeuw. Sinds het einde van de jaren '80 van de vorige eeuw verplichtte de Engelse overheid de politie om hervormingen door te voeren met als doel het vergroten van de effectiviteit en efficiëntie (Gill 2000: 78; Ratcliffe 2008: 33). Dit was het gevolg van een bredere ontwikkeling naar meer marktwerking en een meer bedrijfsmatige aanpak binnen de publieke sector: het zogenoemde *New Public Management*. De overheid moet volgens deze benadering worden gezien als een bedrijf, en dient effectief en efficiënt te werken. Effectief in de zin dat doelstellingen worden behaald en efficiënt in de zin dat dit tegen zo laag mogelijk kosten gebeurt. Dit gold eind jaren '80 en begin jaren '90 voor het eerst ook voor de Engelse politie.

Met name de effectiviteit van het politieoptreden schoot volgens de Britse regering te kort. De tot dan toe gangbare politiemethode stond bekend als de *confessions-method*, vrij vertaald 'verklaringen-methode'. De nadruk van het politiewerk lag bij deze methode op het verkrijgen van bekentenissen of verklaringen van mensen die verdacht werden van misdrijven, hetgeen per definitie reactief is. Bekentenissen en verklaringen zijn immers pas na een gepleegd strafbaar feit mogelijk. De politie werkte reactief en liep als het ware achter de (strafbare) feiten aan.

In de jaren '90 bleven de criminaliteitscijfers stijgen en belangrijke zaken strandden bij het Britse *Court of Appeal* vanwege misbruik van de bestaande bevoegdheden. Met name in de strijd tegen het IRA-terrorisme zijn grote fouten

gemaakt. Onschuldige burgers zijn tot lange gevangenisstraffen veroordeeld omdat de politie bekentenissen had afgedwongen en verdachten had gemanipuleerd.[204] De politie hanteerde verouderde methoden die aan de ene kant niet effectief bleken omdat de criminaliteitcijfers bleven stijgen en aan de andere kant ook nog eens werden misbruikt om te komen tot veroordelingen in zaken die grote publieke bekendheid genoten. Het politieoptreden was voorts inefficiënt omdat het veel geld kostte en weinig resultaat opleverde. Dit leidde tot veel kritiek op het functioneren van de politie en veroorzaakte volgens sommigen zelfs een legitimatiecrisis van de gehele Britse politie (Gill 2000: 78-79; Ratcliffe 2008: 37).

In dezelfde periode ziet een aantal rapporten het licht waarin de ineffectiviteit van de opsporing nog eens pijnlijk wordt benadrukt. Het belangrijkste rapport is '*Helping with Inquiries*' uit 1993 (Ratcliffe 2008: 36-37). Hierin adviseren de opstellers de politie om meer proactief op te treden. De politie moet zich richten op de bekende veelplegers. De oude, reactieve methoden moet zij loslaten. Proactief betekent volgens *Helping with Inquiries* dat de veelplegers intensiever in de gaten worden gehouden en dat ze uit de anonimiteit worden gehaald (Gill 2000: 79). De gedachte is dat omdat veelplegers verantwoordelijk zijn voor een groot aandeel van de criminaliteit, een gerichte aanpak van deze categorie de effectiviteit van politieoptreden zal vergroten. Immers, het in de gaten houden van een veelpleger zodat deze geen strafbare feiten meer kan plegen, zal een grotere preventieve werking hebben dan wanneer de politie zich richt op *first-offenders. Helping with enquiries* en *Policing with Intelligence*, een ander rapport, hebben een belangrijke invloed gehad op de opkomst en acceptatie van IGP: IGP leek het antwoord te zijn van de politieorganisatie op de kritieken uit deze rapporten (Ratcliffe 2008: 37).

Het streven naar (meer) effectiviteit en efficiëntie van de politie is niet beperkt gebleven tot Groot-Brittannië. Ook in Nederland heeft het *New Public Management* inmiddels voeten aan de grond gekregen. In toenemende mate wordt er sinds de jaren '80 van de vorige eeuw gestuurd op *output,* niet in de laatste plaats vanwege een economisering van de collectieve dienstverlening (*New Public Management*) en de zorgen over de gebrekkige effectiviteit van de politie bij de aanpak van de veelvoorkomende en georganiseerde criminaliteit (zie Rosenthal en Van der Torre 2007: 298). Zo worden er sinds een aantal jaren prestatiecontracten tussen de politie en de regering afgesloten waarbij de politie zich verplicht om bepaalde doelstellingen te behalen, zoals het aanbrengen van een vastgesteld aantal verdachten bij het OM. Lukt dit niet, dan leidt deze 'contractbreuk' tot een bepaalde financiële sanctie zoals het beperken van het budget (zie De Kleuver 2007). Ook de Nederlandse politie dient haar geld dus te verdienen.[205] De roep om meer efficiëntie is in Nederland zichtbaar bij de discussie omtrent het beheer van de politie. Het bestaan van vele verschillende computersystemen is bijvoorbeeld al jaren een groot probleem bij de Nederlandse politie. Om meer uniformiteit in de systemen te krijgen, is Voorziening tot Samenwerking Politie Nederland (VtSPN) in het leven geroepen. Deze instantie heeft als doelstelling te komen tot een doelmatiger (efficiënter) beheer van de Nederlandse politie en ontwikkelt hiertoe gestandaardiseerde producten. Medewerkers van de politie zijn met gestandaardiseerde systemen veel minder tijd kwijt dan voorheen, hetgeen efficiënter is, zo is althans de redenering. In hoofdstuk zeven zullen wij echter betogen dat de huidige informatiehuishouding verre van efficiënt is te noemen.

[204] Het gaat om de zogenoemde 'Guildford Four' en 'Birmingham Six' (zie Gill 2000: 79).
[205] Evenals de Britse politie, ziet de Nederlandse politie zich sinds de jaren '80 van de vorige eeuw geconfronteerd met bezuinigingen (zie Fijnaut 2006: 882).

5.2.2 Opkomst georganiseerde criminaliteit

In West-Europa realiseerde men zich in de jaren '80 en '90 van de vorige eeuw dat georganiseerde criminaliteit niet langer slechts een Mediterraans of Amerikaans probleem is: West-Europa heeft ook een actieve criminele 'onderwereld' (Ratcliffe 2008: 22-23).[206] Toen groeide het besef dat er iets aan deze criminaliteitsvorm moet worden gedaan. De specifieke uitdagingen van de georganiseerde criminaliteit vereisen een proactieve aanpak door de politie (zie Gill 2000; Corstens 2008: 258 e.v.; Van der Bel et al. 2009). Criminele netwerken zijn immers zogenoemde gesloten subsystemen die zich actief proberen te onttrekken aan overheidscontrole (zie Gill 2000; Mc Garell et al. 2007). De politie kan hierbij niet reactief zijn en afwachten totdat bepaalde vormen van georganiseerde criminaliteit worden aangebracht door bijvoorbeeld aangiftes: zij moet zelfstandig op zoek gaan naar informatie over deze criminele netwerken. Met andere woorden: de georganiseerde criminaliteit vereist meer nog dan de veelvoorkomende criminaliteit een proactieve aanpak. De heimelijke surveillancemethoden die de politie daarvoor toepast zijn dezelfde als de methoden die de inlichtingen- en veiligheidsdiensten toepassen (zie ook Andreas en Nadelmann 2006: 131). Het gaat dan om het gebruiken van (criminele) informanten, telefoontaps, stelselmatige observatie en dergelijke. Deze surveillance levert bijzonder veel informatie op die vervolgens ook verwerkt dient te worden. Met name bij de bestrijding van de georganiseerde criminaliteit speelt criminaliteitsanalyse vanaf het begin een belangrijke rol. IGP biedt de politie het conceptuele kader om effectief en efficiënt de georganiseerde criminaliteit te bestrijden.

5.2.3 De opkomst van terrorisme

Een belangrijke katalysator voor de ontwikkeling en implementatie van IGP is de opkomst van het islamitisch terrorisme (Mc Garell et al. 2007). Sinds de aanslagen van 11 september 2001 is terrorismebestrijding niet meer weg te denken bij de politie. Omdat terrorismebestrijding primair is gericht op het voorkomen van aanslagen (en dus pas secundair op het aanhouden en vervolgen van verdachten), ligt het zwaartepunt ervan bij het opbouwen en in stand houden van een informatiepositie (Rosenthal et al. 2006: 121-125; Muller en Petit 2008: 291-292). Net als bij georganiseerde criminaliteit is er bij terrorisme sprake van groeperingen die zichzelf actief proberen af te schermen (zie Gill 2000; Rosenthal et al. 2006: 122). Dit vereist van de politie en veiligheidsdiensten dat ze zelfstandig en actief naar relevante informatie zoeken. Daarnaast moeten aanslagen worden voorkomen. Dit betekent dat er dreigingsanalyses en andere analysemethoden worden toegepast die het mogelijk maken om een toekomstvoorspelling te doen. IGP biedt een model volgens welke het informatieproces van de politie kan worden ingericht. Dit geldt met name voor de V.S., waar het streven naar IGP nadrukkelijk wordt verbonden met de uitdagingen van de bestrijding van terrorisme (zie Mc Garell et al. 2007; Ratcliffe 2008: 32).[207]

[206] Peter Gill wijdt in zijn boek over ILP een heel hoofdstuk aan de relatie tussen georganiseerde criminaliteit en de intelligencegestuurde politie (Gill 2000: 58-76).

[207] Volgens O'Connor (2011) is IGP in de V.S. niet echt van de grond gekomen, met name omdat het uitgaat van methoden van *profiling* die zijn gebaseerd op de analyse van veelplegers, wat het minder bruikbaar maakt voor de bestrijding van terrorisme omdat terroristen nu eenmaal relatief weinig voorkomen (in ieder geval te weinig om een profielschets van te maken). O'Connor beoordeelt IGP primair als een middel in de strijd tegen terrorisme en koppelt het daarnaast aan de technologie van *profiling* (zie subsectie 5.2.4).

Kenmerkend voor terrorismebestrijding is overigens de nadruk op het uitwisselen van relevante informatie en kennis tussen verschillende overheidsdiensten, zoals de veiligheidsdiensten en de politie (Rosenthal et al. 2006: 123-124; 189-190).

5.2.4 Schaalvergroting

Politiële opsporing vandaag de dag verschilt aanzienlijk van de traditionele opsporing. Traditioneel was het vrij overzichtelijk: er was een misdrijf, één of meer verdachte(n) en een bepaalde hoeveelheid aan informatie die de rechercheurs dienden te beoordelen. De huidige politie wordt geconfronteerd met een voortdurende schaalvergroting vanwege onder andere (1) een uitbreiding van het strafrecht en (2) een toenemende digitalisering en informatisering van de samenleving.

Er is sprake van een voortdurend uitdijende werking van het strafrecht: steeds meer gedragingen worden door middel van strafbaarstellingen onder de werking van het strafrecht gebracht. Zo zijn er naast de commune misdrijven ook misdrijven die in georganiseerd verband worden gepleegd, misdrijven met een terroristisch oogmerk en technologisch ingewikkelde vormen van criminaliteit zoals *cybercrime*. Veel misdrijven behoeven daarnaast niet eens meer daadwerkelijk te zijn voltooid om toch een strafbaar feit op te leveren (de strafbare voorbereiding, zie voor een beschrijving van deze ontwikkelingen: Boutellier 2005; Borgers 2007; Corstens 2008). Het werkveld van de opsporing omvat dus steeds meer gedragingen van burgers en wordt daarmee steeds groter. Van het strafrecht (en daarmee instanties als de politie en justitie) wordt verwacht dat zij veel meer veiligheid kan bieden dan feitelijk het geval is (Boutellier 2005). Volgens Simon (2007) kan er tegenwoordig worden gesproken van een veiligheidscultuur waarbij het strafrecht wordt gebruikt als instrument om te regeren. Tegenwoordig staat de beleving van veiligheid centraal in de politiek en hierop wordt door politici handig ingespeeld (volgens socioloog Garland gaat het om de 'politisering van criminaliteit en veiligheid', zie Garland 2002: 13-14). De relatief uitgebreide berichtgeving omtrent criminaliteit en terrorisme maakt dat burgers zich onveiliger voelen terwijl de objectieve (in de zin van gemeten) veiligheid juist toeneemt. Een uitbreiding van het strafrecht is vaak het gevolg, met als paradoxaal effect dat meer strafrecht en politieoptreden ook meer gevoelens van onveiligheid lijken te veroorzaken.

Naast een uitbreiding van het strafrecht heeft de politie te maken gekregen met de toenemende digitalisering en informatisering van de gehele samenleving (Schnabel 2004; De Haan 2004; Maas-de Waal 2004: 475-477).[208] Dit leidt niet alleen tot nieuwe vormen van criminaliteit, maar ook tot een groeiende hoeveelheid informatie die betrekking heeft op 'traditionele criminaliteit'. De hoeveelheid informatie die de politie in het kader van haar opsporingstaak te verwerken krijgt is exponentieel gegroeid. Verdachten hebben tegenwoordig niet zelden meerdere telefoonnummers die getapt dienen te worden, gebruiken sms en e-mail om te communiceren en maken gebruik van andere communicatiemogelijkheden die het internet biedt. Dit kan allemaal relevante informatie omtrent strafbare feiten bevatten, en indien iemand is aangemerkt als verdachte, dan zal deze communicatie onderschept moeten worden. Het gaat om informatiestromen die vele malen groter

[208] De informatisering is één van de vijf ontwikkelingen die volgens Schnabel (2004) de langlopende maatschappelijke processen uitmaken. Aan de hand van deze processen kunnen (voorzichtig) uitspraken worden gedaan over mogelijke toekomstige ontwikkelingen op sociaal-maatschappelijk gebied. Het gaat om (1) individualisering, (2) informalisering, (3) informatisering, (4) internationalisering en (5) intensivering. Schnabel noemt dit de 5-i's.

zijn dan vroeger. Daarnaast is op computers veel relevante informatie te vinden. Waar de politie vroeger een aantal ordners van verdachten in beslag nam, is dat nu verworden tot hele computers, harde schijven en andere opslagmedia die in *hard copy* duizenden malen meer papier zouden opleveren dan die oude ordners.

Het is tegen de achtergrond van deze schaalvergroting dat IGP is ontwikkeld. De schaalvergroting leidt aan de ene kant tot een grote uitdaging voor de politie en biedt aan de andere kant ook nieuwe kansen. De grote uitdaging betreft het prioriteren van de werkzaamheden. De politie kan met haar beperkte capaciteit lang niet alle criminaliteitsvormen bestrijden en zal keuzes moeten maken. IGP is in essentie een sturingsconcept waarbij geanalyseerde informatie wordt gebruikt bij te nemen prioriteitsbeslissingen. Op zichzelf is dit niet echt nieuw, ook voordat het IGP werd genoemd werd er al (min of meer) geanalyseerde informatie gebruikt bij het nemen van beslissingen. Maar van criminaliteitsanalyse als discipline en structureel onderdeel van het opsporingsproces was echter geen sprake: de analyses werden door rechercheurs gedaan en er was nauwelijks specifieke kennis van moderne technologieën vereist. Dit kon toen ook nog, omdat de opsporingsonderzoeken relatief overzichtelijk waren. De huidige informatiestromen maken dat het voor de rechercheur niet meer te doen is om zelf alle informatie door te nemen. Het is eenvoudigweg te veel.

De kans wordt gevormd door de nieuwe technologieën die tot op een zekere hoogte nieuwe mogelijkheden bieden om de toenemende informatiestroom te verwerken en te analyseren (Ratcliffe 2008: 23-24).[209] Daarnaast bieden nieuwe technologieën, zoals *datamining*, informatie-filtering en geautomatiseerde *profiling*, de mogelijkheid om aan de hand van geanalyseerde data voorspellingen omtrent trends en ontwikkelingen in criminaliteit te doen. Uit buitenlands onderzoek naar IGP blijkt dat de ontwikkeling van deze nieuwe technologieën zo snel gaat, dat het steeds moeilijker wordt voor leidinggevenden binnen politie en justitie om de door de technologieën geproduceerde analyseproducten te beoordelen (zie Gill 2000; Cope 2004). Zij missen daarvoor de expertise, en vallen daarom in toenemende mate terug op analisten voor de benodigde informatie- en analyseproducten.[210]

5.3 Theoretische verklaringen voor IGP

Belangrijke sociologische theoretische concepten die voor een groot deel de opkomst van IGP verklaren zijn (A) de risicomaatschappij en (B) de surveillance. In deze sectie staan wij allereerst kort stil bij de risicomaatschappij (subsectie 5.3.1). Vervolgens behandelen wij de theorie van surveillance (subsectie 5.3.2). We beschrijven kort op welke wijze deze concepten bijdragen aan het begrip van intelligence en IGP. Het is echter niet onze bedoeling om een complete en uitputtende beschrijving van deze concepten te geven: we schetsen slechts de algemene contouren voor zover deze invloed hebben op het ontstaan van IGP.[211]

---

[209] Zie voor een onderzoek naar de houdbaarheid van het juridisch kader van de politie in het licht van de voortschrijdende ontwikkelingen in de politiële surveillance Schermer (2007). Net als Koelewijn (2009) richt Schermer zich op de relatief nieuwe agenttechnologie: voortdurend en autonoom functionerende softwareprogramma's (Koelewijn 2009: 24).

[210] Uit ons onderzoek blijkt overigens dat dit in Nederland (nog) niet het geval is: de analyseproducten worden weinig gebruikt bij het nemen van beslissingen. Zie hoofdstuk zeven.

[211] Zie voor een recente, uitgebreide behandeling van de risicomaatschappij en de Nederlandse terrorismewetgeving: Van der Woude (2010).

5.3.1 Concept A: De risicomaatschappij

Een risicomaatschappij is een maatschappij die zich in toenemende mate richt op (1) de toekomst en (2) op gevaren. Beide elementen zijn ingrediënten van risico (zie Beck 1992: 33 e.v.; Van der Woude 2010: 52-53). Volgens de Duitse socioloog Ulrich Beck (1992) worden burgers naast de traditionele risico's die het onbedoelde neveneffect van de industriële revolutie waren (zoals werkeloosheid, ziekte en arbeidsongeschiktheid), in toenemende mate geconfronteerd met moderne, technologische risico's. Anders dan de traditionele risico's zijn deze moderne technologische risico's het directe gevolg van menselijk handelen (zie Beck 1992: 22 e.v.; zie ook Van der Woude 2010: 37). Deze moderne risico's zijn (onder andere) (1) moeilijk statistisch te berekenen, (2) zijn niet eenzijdig terug te voeren op een individuele verantwoordelijke en (3) kunnen een catastrofale impact hebben (van der Woude 2010: 37). Terrorisme vormt volgens Beck een risico dat van nature mondiaal is. Een dergelijk risico overstijgt dus landsgrenzen, is moeilijk tot niet in de hand te houden en kan een verwoestend effect hebben op de burgers van een land (Van der Woude 2010: 38). Terrorisme is ongrijpbaar en onvoorspelbaar en heeft mogelijk catastrofale gevolgen. Dit vereist van de overheid een specifieke aanpak: terrorisme dient voorkomen te worden. Daar waar de risicosamenleving in het algemeen uitgaat van het voorkomen en verspreiden van risico's zoals criminaliteit, geldt dit nog meer voor terrorisme. De uitdaging van de risicomaatschappij is hoe met de moderne risico's moet worden omgegaan en hoe ze kunnen worden beheerst (Van der Woude 2010: 41). De sociologische theorieën van Beck (en Giddens) zien met name op de veranderende verhoudingen tussen bepaalde maatschappelijke klassen. Wij laten dit verder buiten beschouwing. Voor ons onderzoek is met name de focus op toekomstige gebeurtenissen van belang. Criminaliteit is één van de potentiële risico's waar de risicosamenleving op is gericht (Hudson 2003).

In de huidige samenleving is er weinig ruimte voor veiligheidsrisico's, en waar deze worden waargenomen, dienen ze zoveel mogelijk voorkomen te worden. Nauw verwant aan de risicosamenleving is de term 'veiligheidscultuur' zoals die geïntroduceerd is door Garland (hij spreekt van een '*culture of control*', zie Garland 2002). Volgens hem heeft het strafrecht in de jaren '70 van de vorige eeuw een radicale verandering doorgemaakt waarbij de tot dan toe geldende resocialisatiegedachte plaatsmaakte voor een bescherming van de meerderheid van de samenleving die zich normconform gedraagt (zie Van der Woude 2010). In een veiligheidscultuur worden de overheid en de samenleving geconfronteerd met een 'nieuw criminologisch dilemma': het bestaan van hoge criminaliteitsgegevens als normaal sociaal gegeven binnen een open, complexe en welvarende samenleving gecombineerd met het besef dat de rechtsstaat en de overheid slechts een beperkt antwoord kunnen geven op de bestaande criminaliteitsproblemen (Van der Woude 2010: 50). Dit criminologisch dilemma heeft ertoe geleid dat overheden veranderingen in de criminaliteitsbestrijding moesten doorvoeren. Er zijn twee beleidsstrategieën naast elkaar tot stand gekomen: (1) de aanpassingsstrategie en (2) de ontkenningsstrategie. Beide hebben een belangrijke invloed op de ontwikkeling van IGP gehad. De aanpassingsstrategie is gericht op de actoren die zijn betrokken bij de criminaliteitsbestrijding. Door middel van reorganisaties moet het justitiële apparaat worden hervormd en efficiënter en effectiever worden gemaakt (Van der Woude 2010: 51). Het gaat hierbij om organisatorische aanpassingen van de (overheids)organisaties die zijn betrokken bij de bestrijding van criminaliteit. IGP is een voorbeeld van een dergelijke hervorming. De tweede strategie (de

ontkenningsstrategie) is gericht op politici en het grote publiek. Door middel van beleidsplannen probeert de overheid weer grip te krijgen op het criminaliteitsprobleem. De beleidsplannen zijn met name bedoeld om het publiek gerust te stellen en zijn symbolisch van aard. Met een daadwerkelijke bestrijding van criminaliteit hebben ze weinig te maken (Van der Woude 2010: 51). De tweede benadering ligt aan de basis van risicojustitie: een criminaliteitsbestrijding die in het teken staat van het bestrijden van criminaliteit door het justitiële systeem preventief te richten op bedreigingen en risico's (Hudson 2003). Een concrete verdenking van een strafbaar feit vormt dan geen grondslag meer voor optreden van politie en justitie; het beleid gaat uit van generalisaties en baseert hierop risicoprofielen van mogelijke (criminele) gevaren. Het anticiperen op mogelijke toekomstige criminaliteit en het voorkomen daarvan vormen belangrijke kenmerken van de laatmoderne (strafrechtelijke) criminaliteitsbestrijding. De risicobenadering vereist van de politie dat zij haar aanpak aanpast: reageren op criminaliteit is niet meer voldoende, de politie moet actief informatie gaan verzamelen.

5.3.2 Concept B: Surveillance

De theorie van de risicosamenleving verklaart *waarom* de politie overgaat op een intelligence-benadering. Het verklaart echter nog niet *hoe* intelligence werkt. Het concept van surveillance helpt ons te begrijpen hoe intelligence werkt.

Surveillance ziet op de relatie tussen kennis en macht (Gill en Phythian 2006: 31). Kennis ziet op het verzamelen, opslaan en verwerken van informatie. Macht ziet met name op de supervisie van menselijk gedrag. Ons onderzoek richt zich op het eerste kenmerk (kennis). Uiteindelijk zal de kennis leiden tot een actie: er wordt macht uitgeoefend. Kennis en macht staan in een nauwe relatie tot elkaar: in zekere zin is kennis macht (Schermer 2007: 2). Het enkele gegeven dat er informatie wordt verzameld en kennis wordt geproduceerd heeft een impact op een populatie en kan leiden tot aanpassing van gedragingen (Gill en Phythian 2006: 33; Schermer 2007: 8-9). Volgens Gill en Phythian (2006) biedt de theorie van surveillance een verklaring voor modern bestuur. Surveillance is de kerntaak van de politie geworden (Ericson en Haggerty 1996: 41-42). De toenemende focus van politiediensten (en overigens ook inlichtingen- en veiligheidsdiensten) op surveillance, maakt dan ook dat er steeds meer kan worden gesproken van een surveillancemaatschappij (Ericson en Haggerty 1996; Lyon 2006; Schermer 2007). Het schrikbeeld van een dergelijke maatschappij wordt gevormd door Foucault's Panopticon[212]: een alwetend overheidsapparaat dat alles in de gaten houdt.[213]

[212] Inmiddels lijkt het concept van de Panopticon enigszins achterhaald en verouderd. Het gaat teveel uit van een monolithische benadering van de surveillance en geeft geen verklaring voor technologische en sociale ontwikkelingen die de surveillance hebben veranderd (Bogard 2006; Schermer 2007: 39). Surveillance vindt plaats in een surveillance-assemblage: een rhizomatisch netwerk van verschillende partijen en individuen die surveillance verrichten. Deze assemblage omvat meer dan een afgebakende organisatie zoals de politie: het ziet op materiële processen (zoals machines, technologieën, individuen, organisaties) en immateriële processen (zoals die plaatsvinden in sociale categorisatie en in collectieve mentale representaties van bijvoorbeeld risico's) (Bogard 2006: 101-106).

[213] In de huidige samenleving vindt de surveillance steeds vaker digitaal plaats. Een veelgebruikte term voor deze vorm van controle is '*dataveillance*'. De mens heeft vanwege de digitalisering (of informatisering) een digitale dubbelganger gekregen: de code in de zin van een reeks ééntjes en nulletjes. De code is als het ware de digitale variant van het individu en geeft toegang tot bepaalde ruimtes en maakt bepaalde handelingen (on)mogelijk. De Panoptische blik richt zich nu niet meer op het lichaam van individuen, maar op de codes. In de woorden van Simon: "(…) *in dataveillance the object of control is simply the digital representation of the body*" (2005: 15).

Veiligheidsdiensten hebben te maken met een informatieprobleem: "*Faced with uncertainty, risk, feelings of insecurity, or in search of some other goal, all human entities face a 'knowledge problem' and seek information that (they hope) will reduce uncertainty, enable them to address their vulnerabilities, and advance their interests*" (Gill en Phythian 2006: 30). De kern van het inlichtingenwerk, of dit nu door veiligheidsdiensten of politiediensten wordt verricht, wordt gevormd door informatieproblemen. Het gaat bij onzekerheden, risico's en gevoelens van onveiligheid altijd om toekomstige gebeurtenissen. De organisaties hebben informatie nodig om deze gevoelens weg te nemen, maar vanwege het open karakter ervan (het betreft immers de toekomst, en die is in alle gevallen onzeker), is het nooit duidelijk wanneer er voldoende informatie is. Zeker weten kan nooit in die gevallen, dus zijn mensen (en organisaties) aangewezen op het maken van inschattingen over mogelijke toekomstige gebeurtenissen. Dit is in meer of mindere mate altijd een vorm van gissen. Meer informatie betekent echter ook een beter geïnformeerd gissen; dit leidt tot een onverzadigbare honger naar informatie. Immers, meer informatie kan nieuwe bedreigingen aan het licht brengen, die de informatiebehoefte van mensen verder aanwakkert. Zo zitten we in een mogelijke vicieuze cirkel.

Het informatieprobleem is dus een permanent probleem en zal in abstracto nooit worden opgelost. De informatiezucht en het bijbehorende permanente informatieprobleem zijn ook van belang voor de verhouding tussen de de veiligheidsdiensten en de politiële inlichtingendienst: beide organisaties zullen de andere partij zien als een relevante informatiebron. In hoofdstuk twee hebben we echter betoogd dat bureaucratische organisaties zoals een veiligheidsdienst en de politiële inlichtingendienst vanwege uiteenlopende redenen een verregaande mate van geheimhouding betrachten. De honger naar informatie gecombineerd met de afscherming en geheimhouding leveren ingrediënten voor inter-organisatorische conflicten.

De steeds belangrijker wordende rol van ICT en de immer verdergaande digitalisering van de samenleving gecombineerd met de ontwikkeling in de richting van een risicomaatschappij leidt ertoe dat het werk van de politie meer dan ooit berust op het opbouwen en in stand houden van een informatiepositie (Cope 2004: 190-191). De implementatie van intelligence in de context van de politie is een logische stap: IGP is het werkproces van de politie in een risicomaatschappij. In de volgende sectie behandelen wij dit concept zoals het binnen de politie vorm heeft gekregen.

5.4 IGP

Volgens de hoofdanalist van de Kent Constabulary (zoals gezegd het politiekorps waar IGP zou zijn bedacht, zie subsectie 5.2.1) is IGP als volgt te omschrijven: "*At its most fundamental, intelligence led policing involves the collection and analysis of information to produce an intelligence end product designed to inform police decision making at both the tactical and the strategic level. It is a model of policing in which intelligence serves as a guide to operations, rather than the reverse. It is innovative, and, by some standards, even radical, but is predicated on the notion that a principal task of the police is to prevent and detect crime rather than react to it*" (Jansen 2001: 11). Het was onder meer een reactie van de politie op toenemende kritiek op het functioneren van de politiediensten aldaar (Ratcliffe 2008: 33-40). IGP werd al gauw overgenomen door andere politiediensten en werd met name toegepast bij de opsporing van de zware en georganiseerde criminaliteit. Onder de noemer

National Intelligence Model werd het hele Britse opsporingsproces gereorganiseerd volgens de principes van IGP. Na de invoering van het concept claimden de Britse korpsen succes na succes, hetgeen overheden en politiediensten in het buitenland niet ontging. Ook de Nederlandse politie omarmde IGP als het nieuwe antwoord op criminaliteitsproblematiek (Jansen 2001; Huisman et al. 2005; Van Calster en Vis 2008). De nadruk binnen IGP op criminaliteitsbestrijding wordt gezien als één van de verklaringen voor de populariteit van het concept bij politieorganisaties: dit zou appelleren aan het gewenste imago van de *crimefighters* en boevenvangers. Inmiddels wordt IGP breder uitgelegd dan als louter een concept voor de opsporing. Het concept IGP moet beleidsmensen in staat stellen niet alleen de opsporing, maar het gehele politiewerk grondig te hervormen. Er werd in Nederland een stuurgroep (ABRIO; 'Aanpak Bedrijfsvoering Recherche, Informatie en Opleiding')[214] ingesteld die de opdracht kreeg allereerst te onderzoeken of het Nederlandse politiebestel klaar was voor de invoering van IGP en zo nee, wat er aan gedaan kon worden om dit wel mogelijk te maken (Jansen 2005: 48-56). In 2010 moest de gehele Nederlandse politie volgens de uitgangspunten van IGP werken. Inmiddels lijkt ieder onderdeel van de politie het concept IGP te hebben omarmd: het is een politiebrede ontwikkeling. Sommigen noemen het zelfs al een nieuw paradigma voor politiewerk (Ratcliffe 2008).

Sinds de opkomst van IGP kenmerkt het concept zich echter door onduidelijkheid. In de politiepraktijk wordt het voorgesteld als dè oplossing voor vrijwel alle problemen waarmee de moderne politie zich ziet geconfronteerd. De in de praktijk gehanteerde benaderingen en definities scheppen echter geen duidelijkheid in de aard en achtergronden van IGP. Al eerder kreeg de Nederlandse stuurgroep die was belast met het implementeren van het concept bij de Nederlandse politiekorpsen naar eigen zeggen een paar krachtige uitspraken van *Chief Constable* van Kent, Sir David Philips, te horen: "*Intelligence led policing is not a philosophy, but a practicality*" en "*if you want to attack crime, you have to write the handbook of crime. Only then you are in business*" (Jansen 2002: 11). Dergelijke terminologie is aansprekend, maar inhoudelijk is het weinig functioneel en draagt het niet of nauwelijks bij tot een beter begrip omtrent het concept IGP. Een beter bruikbare en recente definitie van IGP is afkomstig van Ratcliffe: "*intelligence led policing is a business model and a managerial philosophy where data analysis and crime intelligence are pivotal to an objective, decision-making framework that facilitates crime and problem reduction, disruption and prevention through both strategic management and effective enforcement strategies that target prolific and serious offenders*" (2008: 89). Volgens Ratcliffe is IGP dus een sturingsmodel waarbij criminaliteitsanalyse leidt tot een objectieve besluitvorming. Sommigen zien IGP dus vooral als een sturingsconcept waarbij criminaliteitsanalyses aan de basis liggen van beslissingen (zie ook NCIS 2000; Meesters en Niemijer 2000; ABRIO 2003; Ratcliffe 2008).

Anderen zien IGP als veel meer dan een sturingsconcept, en benoemen een normatief probleem: "*(ILP) reeks of secret service, spy agency work- the capital 'I' in 'Intelligence*" (Zaccardelli 2005 in Brodeur 2007: 29). Volgens deze critici is IGP een bedreiging voor de burgerlijke vrijheden, zelfs zodanig dat "*the winds of history are blowing (...) towards authoritarianism*" (Sheptycki 2005). Volgens deze auteurs is het

[214] De stuurgroep valt onder de Raad van de Hoofdcommissarissen. De werkzaamheden van ABRIO worden dan ook onder de verantwoordelijkheid van de Raad verricht.

wachten op *Big Brother* (zie ook Vedder, Van der Wees en Koops 2006). De zienswijzen en meningen omtrent IGP lopen dus uiteen.

In deze sectie behandelen wij de uitgangspunten van het concept IGP zoals het is vormgegeven door de politie. Het eerste uitgangspunt is 'het opbouwen en in stand houden van een informatiepositie' (subsectie 5.4.1). Het tweede uitgangspunt is een proactieve werkwijze en preventieve criminaliteitsbestrijding (subsectie 5.4.2). Hierna behandelen wij uitgangspunt drie, te weten effectieve sturing van het politiewerk (subsectie 5.4.3). Het vierde en laatste uitgangspunt van IGP is het delen van informatie (subsectie 5.4.4). Na de behandeling van de kenmerken van IGP, beantwoorden wij de vraag of IGP echt nieuw is, of dat het oude wijn in nieuwe zakken betreft (subsectie 5.4.5). Vervolgens beschrijven wij Ratcliffe's 3-i model, dat weer een aantal andere elementen van IGP behandelt (subsectie 5.4.6). Als laatste behandelen wij wat er binnen het concept IGP doorgaans met 'intelligence' wordt bedoeld (5.4.7).

5.4.1 Verwerken van informatie: de informatiepositie

Het eerste uitgangspunt van IGP is (eenvoudig geformuleerd) dat de politie moet weten wat er in de samenleving speelt. Zij vormt daartoe een beeld van de externe wereld (de maatschappij). Hiervoor heeft zij kennis en informatie nodig omtrent diverse veiligheidsvraagstukken. Het idee is dat alle informatie die in de politieorganisatie aanwezig is van belang kan zijn voor effectieve opsporing en preventie van criminaliteit. Overigens geldt dit niet alleen voor politie-informatie: ook informatie van externen kan van belang zijn voor de bestrijding van criminaliteit. IGP biedt de politie een conceptueel kader voor het verwerken van de toenemende informatiestromen. Essentieel voor de opbouw en het in stand houden van een politiële informatiepositie is de discipline van de criminaliteitsanalyse. Criminaliteitsanalyse is echter niet specifiek voorbehouden aan IGP. Het is een discipline die al in de jaren '70 van de vorige eeuw in Nederland opduikt en sinds de jaren '80 echt voeten aan de grond heeft gekregen (Fijnaut en Moerland 2000: 23). Weliswaar kende criminaliteitsanalyse in de jaren '90 een dip in de ontwikkeling, maar dat neemt niet weg dat er al aan bepaalde vormen van criminaliteitsanalyse werd gedaan voordat IGP was ontwikkeld.

5.4.2 Proactieve werkwijze en preventieve criminaliteitsbestrijding

Het tweede uitgangspunt van IGP is de proactieve werkwijze en de preventieve aanpak van criminaliteit. Dit gebeurt met name door het politieoptreden te richten op veelplegers (zie Gill 2000; Ratcliffe 2008). Daarmee zou het politieoptreden effectiever worden. De traditionele politiële werkwijze van het reageren op criminaliteit is niet langer voldoende: de politie dient ook op criminaliteit te anticiperen. In tegenstelling tot *community policing* wordt daarom binnen IGP met name criminaliteitsbestrijding centraal gesteld: het gaat verder dan de reactieve opsporing van strafbare feiten.[215] Overigens zijn proactiviteit en preventie ook niet

[215] Overigens is IGP onderhevig aan het fenomeen van *netwidening*: het concept wordt steeds breder toegepast op verschillende aspecten van het politiewerk. Door de *netwidening* verliest IGP echter steeds meer onderscheidende kenmerken: het is immers op vrijwel al het politiewerk van toepassing. Zie ook De Hert, Huisman en Vis (2005: 371-372)

echt nieuw voor de politie. Al in 1829 beschreef Sir Richard Maine (1829)[216] de primaire taak van de politie als volgt: "*It should be understood at the outset, that the principal object of an efficient police is the prevention of crime. To this great end, every effort of the police is to be directed. The security of persons and property, the preservation of public tranquility and all other objects of a police establishment will thus be better affected than by the detention and punishment of the offender after he has succeeded in committing the crime.*" Preventie is dus altijd al een belangrijke doelstelling van de politie geweest, alhoewel de 19e eeuwse benadering van preventie breder is dan die van de 20e en 21e eeuw.[217]

Proactief politiewerk is ook niet nieuw voor landen die al langer kampen met veel georganiseerde criminaliteit. In dergelijke landen, zoals de V.S. en Italië, maakten opsporingsdiensten al ver voor het ontstaan van IGP gebruik van werkwijzen die wij vandaag de dag zouden scharen onder de noemer van intelligence en IGP. Een voorbeeld is de FBI, die al in de jaren '30 van de vorige eeuw heimelijke surveillance toepaste in de strijd tegen de georganiseerde criminaliteit en vervolgens de relevante criminele netwerken analyseerde (Jeffreys-Jones 2007). Het verzamelen en analyseren van inlichtingen speelt bij het bestrijden van georganiseerde criminaliteit altijd een essentiële rol, of dit nu gebeurt in het kader van een concept als IGP of in een meer traditionele benadering van de opsporing. Dit neemt echter niet weg dat proactiviteit een belangrijk uitgangspunt van IGP is. IGP is een concept waarmee een proactieve werkwijze een structureel onderdeel is van het politiewerk in het algemeen.

5.4.3 Effectieve sturing

Het derde uitgangspunt is dat IGP bedoeld is om de politie te sturen: "*het is primair een filosofie over het gebruik van informatie voor het sturen van de organisatie of, preciezer, van wat politiemensen doen*" (Stol 2007: 387). Het is een hiërarchisch model en gaat uit van *top down* management. De politieleiding bepaalt de prioriteiten en stuurt binnen IGP actief de politiemedewerkers die lager in rang staan aan. Door middel van analyse krijgt de politie een beeld van de problemen die voor haar relevant zijn en op basis van analyseproducten worden gericht projecten voorbereid. Daar waar relevante informatie ontbreekt, wordt gericht naar die informatie gezocht.

---

[216] De eerste '*Commissioner of the Metropolitan Police*' in Londen. Geciteerd uit een toespraak van Sir John Stevens, de '*Commissioner of the Metropolitan Police*' in Londen van 2001 (*2nd world conference on Modern Criminal Investigation, Organized Crime and Human Rights*, ICC, Durban, 3-7 december 2001).

[217] De opvatting van Sir Richard Maine stamt namelijk uit een periode waarin politiewerk nog werd benaderd vanuit de '*Polizeigedanke*', een onderdeel van de 18e en 19e eeuwse Duitse wetenschappelijke discipline van de '*Polizeiwissenschaft*'. Dit is een vorm van bestuurskunde waarin wordt gekeken naar een zodanige inrichting van het openbaar bestuur dat de algemene welvaart van burgers en de staat het meest gediend is ((Hoogenboom 1994: 18). Deze *Polizeigedanke* kent twee componenten: een welvaartscomponent en een veiligheidscomponent die wederkerig met elkaar zijn verbonden. Onder invloed van de toenemende macht van de burgerij en het Verlichtingsdenken wordt de brede opvatting van de *Polizeigedanke* steeds verder ingeperkt. De veiligheidscomponent *w*int het door de eeuwen heen van de welvaartscomponent (Hoogenboom 1994:19). De betekenis die destijds aan preventie werd toegekend is dan ook breder dan de huidige: preventie stond tegenover repressie en is het equivalent van welzijnstaken en justitiële taken (Hoogenboom 1994: 21). De huidige betekenis wijkt hiervan af. Vandaag de dag is het niet langer denkbaar dat de politie zich bemoeit met de welvaart van de burgers: de veiligheid is de enige doelstelling van de politie. Preventie anno 2012 is dan ook primair het voorkomen van criminaliteit door middel van veiligheidsgerelateerde maatregelen, en niet welvaart verhogende maatregelen.

Dit houdt bijvoorbeeld in dat agenten de straat op worden gestuurd met een specifieke opdracht of dat er gericht wordt gezocht naar informanten die op specifieke vragen een antwoord kunnen geven. Er wordt dus zowel gestuurd op als met informatie.[218] Als de leidinggevenden van een dienst voldoende informatie hebben, kan er gericht worden opgetreden. Omdat er een voortdurende stroom van informatie binnenkomt, is dit een doorgaand proces, een cyclus. Het werkproces van IGP is daarmee dus grotendeels gelijk aan de intelligence cyclus uit hoofdstuk 2 (zie ook subsectie 5.6.1).

5.4.4 Delen van informatie

Het vierde uitgangspunt van IGP is dat informatie meer gedeeld moet worden door de verschillende politiediensten: "*for this model to work effectively, intelligence has to flow freely on and on between all the levels and interchange smoothly between agencies*" (Sheptycki 2004: 311). Aan de basis van dit idee ligt de notie dat het beste intelligence systeem een piramidestructuur heeft met een brede basis bij de korpsen waar vanuit veel informatie omhoog stroomt door een steeds smaller wordende structuur met uiteindelijk in de top de hoogste hiërarchische leiding op nationaal en internationaal niveau (Stevens 2001: 5; Sheptycki 2004: 311). Informatie moet dus zowel horizontaal (tussen verschillende korpsen) als verticaal (hoger in de hiërarchie van de politieorganisatie) kunnen bewegen. Dit vereist dat er zo weinig mogelijk barrières zijn die de informatiestromen belemmeren, en de cultuur van *need to know* is een voorbeeld van een dergelijke barrière die zal moeten worden geslecht (zie sectie 2.6 voor een uitgebreide behandeling van geheimhouding).

In Nederland wordt er door veel korpschefs de nadruk gelegd op het stroomlijnen van het informatieproces en de uitwisseling van informatie, omdat dit de prestaties van de politie zou verbeteren (Boin et al. 2007: 324). Het nieuwe adagium van de politie is 'delen tenzij…', wat ook bekend is geworden als het '*need to share*-streven' (zie NIM 2008; 2011). Binnen IGP moet er dus zoveel mogelijk informatie worden gedeeld. In subsectie 5.5.2 zullen we hier dieper op in gaan.

5.4.5 IGP: oude wijn in nieuwe zakken?

Volgens de genoemde vier uitgangspunten is IGP dus een model waarbij (1) criminaliteitsanalyse leidt tot de opbouw en instandhouding van een informatiepositie welke (2) de besluitvorming faciliteert en waarbij (3) informatie zoveel mogelijk wordt gedeeld, dit alles ten behoeve van (4) een proactieve werkwijze en preventieve aanpak van criminaliteit (en terrorisme). Er zijn echter ook andere zienswijzen mogelijk. Wij noemen hieronder nog het 3i-model van Ratcliffe als alternatief model (zie 5.4.6). Overigens wijzen wij de lezer er op dat wij ook een andere definitie van IGP hanteren, zie daarvoor hoofdstuk één. Hieronder staan wij kort stil bij de vraag: wat is er eigenlijk nieuw aan IGP?

De vier hierboven genoemde uitgangspunten van IGP zijn niet specifiek voorbehouden aan het concept IGP en bestaan op zichzelf al langer dan IGP (Zie ook: Stol 2007: 387). Het huidige politiewerk kan echter niet meer worden vergeleken met dat van vroeger. Alles is grootschaliger en de specifieke kennis omtrent bepaalde personen is met name in de grote steden niet bij iedere agent aanwezig. IGP is in dit

[218] Hiermee wordt overigens niet bedoeld dat de politie informanten stuurt: dit is niet toegestaan. Zie voor de regels omtrent het runnen van informanten door de CIE hoofdstuk vier.

opzicht eigenlijk een poging om de 'boerenlogica' van vroeger om te vormen in een concept dat voldoet aan de eisen van de moderne tijd en tegemoet komt aan de eerder beschreven schaalvergroting (zie subsectie 5.4.3). Wat dus nieuw is aan IGP, is de schaal waarop over intelligence wordt gedacht. Het is namelijk de bedoeling (van de Nederlandse Raad van Korpschefs) dat de gehele politie volgens IGP gaat werken. De samenleving van de 21e eeuw is niet vergelijkbaar met die van de 19e en 20e eeuw, en dat geldt ook voor de criminaliteit. Informatiestromen zijn groter en complexer dan voorheen, en nieuwe technologieën zorgen aan de ene kant voor nieuwe oplossingen, maar aan de andere kant ook voor nieuwe problemen. De samenleving is 'plat' in de zin dat er bijna geen plekken in de wereld onbereikbaar zijn. Dit zorgt er bijvoorbeeld voor dat criminaliteit zich meer dan voorheen internationaal kan manifesteren. De politieorganisatie ziet zich geconfronteerd met een veranderde wereld en dient zich aan te passen. IGP is het concept waarmee de politie de uitdagingen van vandaag de dag (de schaalvergroting) tegemoet meent te kunnen treden. IGP verschilt dus van deze traditionele intelligence methoden in die zin dat het tot een standaard werkwijze is geworden van de gehele politie.

5.4.6 Ratcliffe's 3i-model

Een andere belangrijke benadering van IGP is die van Ratcliffe (2008). We zullen deze benadering apart behandelen omdat deze in belangrijke opzichten afwijkt van andere benaderingen van IGP. Ratcliffe ziet IGP als een '3i-model', waarbij de 3 i's staan voor: interpretatie, invloed en impact: "*all three i components of the 3-i model must exist if true intelligence led policing is to take place. The crime intelligence analyst must* interpret *the criminal environment, the analyst must then use that intelligence to* influence *the thinking of decision-makers, and decision-makers must direct resources effectively in order to have a positive* impact *on the criminal environment.*" (Ratcliffe 2008: 112). Het eerste element interpretatie hebben wij in subsectie 5.4.1 behandeld. Het laatste element impact hebben wij in subsectie 5.4.2 al behandeld. Interpretatie ziet op het werk van de criminaliteitsanalyse en door middel van effectieve sturing dient de politie efficiënt in criminele processen in te grijpen. Wat nieuw is in de benadering, is de beïnvloeding van de besluitvormers (invloed). Volgens Ratcliffe dient een analist de beslissers (de hogere politieleiding) te begeleiden en eigenlijk te onderwijzen in de mogelijkheden van intelligenceproducten (Ratcliffe 2008: 154). Intelligence is vaak het enige objectieve element dat bij besluiten wordt betrokken en dit dient ook als zodanig op waarde te worden geschat (Ratcliffe 2008: 155). Het vereist van de analist dat hij continu rekening houdt met de druk die beslissers ervaren in een politiek-bestuurlijke of maatschappelijke context. Het betekent ook dat een analist zich ervan bewust moet zijn dat de beslissers behoefte hebben aan bondige, *to the point* analyses (Ratcliffe 2008: 154).

Ratcliffe's model is waardevol voor het beoordelen van de praktijk van IGP en met name de praktijk van de criminaliteitsanalyse. In de politiewereld werd dit nieuwe model niet automatisch geaccepteerd (zie Cope 2004). Het is goed dat analisten zich bewust zijn van de contextuele aspecten van politiële besluitvorming. Hier heeft Ratcliffe dus een belangrijk punt. Er schuilt echter ook een gevaar in zijn benadering. De vraag is namelijk in hoeverre intelligence nog objectief kan zijn als de analist al rekening gaat houden met mogelijke besluitvorming. Is analyse objectief of niet objectief als het plaatsvindt met inbegrip van allerlei elementen zoals druk van buitenaf in het interpretatieproces? Wellicht zou een oplossing zijn dat analisten in de

interpretatiefase geen rekening houden met de contextuele aspecten van besluitvorming, en dat ze dit pas doen op het moment dat ze de resultaten presenteren. Maar deze benadering schept een illusoir beeld van objectiviteit. Het enkele feit dat een analist in een latere fase rekening moet houden met andere zaken dan de objectieve feiten (voor zover politiedata objectief zijn, dat is evenwel een andere discussie), zal doorwerken in het analyseproces zelf. Dat de onderliggende analyse objectief tot stand is gekomen is niet relevant: de presentatie van het analyseproduct is de intelligence, en die is niet meer objectief of waardevrij. Wanneer analisten bewust invloed uit proberen te oefenen op besluitvorming, is de objectiviteit van intelligence sterk verminderd. Overigens is het element invloed niet onderscheidend voor IGP, maar het geldt voor iedereen die betrokken is in het politieproces. Wij zien Ratcliffe's element van invloed dan ook niet als een specifiek onderdeel van IGP. Het is echter wel van belang bij de behandeling van de implementatie van IGP in de praktijk en komt daarom terug in hoofdstuk zeven (sectie 7.5).

5.4.7 Intelligence

We hebben in sectie 1.2 IGP gedefinieerd als 'de implementatie van het concept van intelligence in de context van de politiële bestrijding van criminaliteit' (definitie twee). De vraag die nu rijst, is wat wordt bedoeld met intelligence. Er zijn veel verschillende visies op wat intelligence precies is (zie Warner 2002; Phythian en Gill 2006).

Intelligence kan *grosso modo* op twee manieren worden benaderd. Aan de ene kant wordt er het proces van informatieverzameling mee bedoeld en aan de andere kant het eindproduct van dat proces (McDowell 1995: 1). Als proces wordt intelligence ook wel beschreven als een discipline danwel kunstvorm: "*It's the art of gathering and giving meaning to information*" (Meesters en Niemeijer 2000: 305). Een algemene en basale definitie is "*verwerkte informatie, waarbij het verwerken als doel heeft de informatie te interpreteren en een betekenis te geven*" (McDowell 1995: 1). Er zijn dus verschillende benaderingen mogelijk, waarbij een keuze voor een bepaalde benadering gevolgen heeft voor een bij een analyse te gebruiken conceptueel kader. Het is daarom belangrijk om kort stil te staan bij de verschillende benaderingen en te beargumenteren waarom wij voor een specifieke benadering hebben gekozen.

In deze subsectie behandelen wij (A) de door de politie gehanteerde benadering van intelligence, (B) beargumenteren wij waarom deze benadering tekort schiet en (C) herhalen wij de door ons gehanteerde definitie.

A: De politiebenadering: de piramidale visie

Binnen de politie benadert men intelligence met name als een product van het analyseproces. Intelligence staat daarom in een hiërarchische verhouding tot andere modaliteiten van informatie. Deze politiebenadering noemen wij de 'piramidale visie'.

In het dagelijkse spraakgebruik binnen de politie worden de termen 'data' en 'informatie' vaak door elkaar gebruikt, maar feitelijk verschillen ze van elkaar. De termen 'data', 'informatie', 'kennis' en 'intelligence' worden meestal in een logische trits geplaatst en staan in een hiërarchische verhouding tot elkaar; een

piramidestructuur (zie Davenport en Prusack 1998: 1-7).[219] Deze productbenadering past binnen een steeds dominanter wordende ICT-visie op werkprocessen binnen de politie (en overigens ook daarbuiten). Data, informatie, kennis en intelligence zijn in dit opzicht vatbaar voor opname in computersystemen; ze zijn te manipuleren. In deze subsectie behandelen wij de verschillende elementen van de piramidale visie op intelligence. Binnen de politie wordt er vaak alleen maar gesproken van data, informatie, kennis en intelligence. Er zijn echter meer onderdelen te onderscheiden. Van de Herik (1993) onderscheidt de volgende modaliteiten: (1) ruwe data, (2) data, (3) gegevens, (4) informatie, (5) kennis, (6) intuïtie, (7) normen, (8) waarden en (9) intelligence in de zin van intelligentie. Wij lichten deze modaliteiten kort toe.

Ruwe data staan het laagst in de hiërarchie en zijn 'losse gegevens'. Het kan gaan om bepaalde getallenreeksen of andere gegevens waar nog geen bewerking van is gemaakt. Data is overal om ons heen; alles wat we waarnemen is een vorm van ruwe data. Het vormt dan ook de brede basis van de piramidale visie. Indien ruwe data wordt geschoond (bijvoorbeeld in een filteringsproces), ontstaat data.

Data bestaan uit feiten die door mensen zijn vastgelegd. Het kan gaan om lange getallenreeksen waar een bepaalde orde in is aangebracht. Op zichzelf zegt deze ordering nog niets over wat de getallen betekenen: het kan een tijdsordening zijn, of een telefoonnummer. We staan nu op een tweesplitsing: (A) we kunnen uit de data gegevens halen (een kleine deelverzameling van de data) om iets 'te bewijzen' en daarmee onze kennis te vermeerderen; (B) we kunnen de data die we hebben van betekenis voorzien (dat wil zeggen: we interpreteren de data). Geïnterpreteerde en in een context geplaatste data noemen we informatie. Niet-geïnterpreteerde data heeft geen directe waarde en kan als 'dode materie' worden gezien. Tegenwoordig bestaat de neiging om veel data en ook veel ruwe data te bewaren omdat die mogelijk later in het intelligenceproces gebruikt kunnen worden (bijvoorbeeld bij *cold cases* waarbij bijvoorbeeld kleren met mogelijke DNA-sporen worden bewaard. De DNA-analyse heeft interpretatie mogelijk gemaakt en vanwege de ontwikkelingen op het vlak van DNA-analyse zal dit in toenemende mate het geval worden). Het is dus steeds makkelijker geworden om data op te slaan en een lange tijd te bewaren.

Een stap hoger in de hiërarchie dan informatie staat kennis. Kennis is informatie die van een context is voorzien. De analyse van de informatie leidt in combinatie met de context tot kennis omtrent een bepaalde problematiek (Minnebo 2004: 26). De productie van kennis is te vergelijken met de academische wetenschap. Door het toepassen van onderzoeksmethoden komt men tot een gedachte of voorstelling van waargenomen fenomenen. Door middel van kennis oriënteren mensen zich in de werkelijkheid (Stol 2007: 382). Kennis geeft antwoord op de hoe- en waarom vragen.

Na kennis volgt intuïtie. Dit is kennis die onbewust of onderbewust is. In de literatuur over informatiemanagement wordt vaak gesproken over niet-tastbare kennis (*tacit knowledge,* of 'impliciete kennis') (Davenport en Prusak 1998; Nonaka 1998; Dalkir 2005). Attitude en ervaringskennis behoren tot de fase van intuïtie. Deze vorm van kennis is veel moeilijker in computersystemen te vatten en wordt zelden betrokken bij discussies omtrent IGP (zie Van Calster en Vis 2008: 82). Dit is onzes inziens onterecht, en we zullen hier in hoofdstuk zeven nog verder op in gaan.

[219] Davenport en Prusack noemen intelligence niet, maar hebben het over '*information ready for action*'. Zij richten zich echter op het bedrijfsleven en de rol van een kennisorganisatie in deze specifieke context. Het is trouwens opvallend hoeveel overeenkomsten er zijn tussen kennisorganisaties in het bedrijfsleven en de intelligence-diensten.

Intuïtie wordt weer gevolgd door normen. Normen zijn bepaalde leef- en gedragsregels waaraan mensen zich dienen te houden. Een voorbeeld hiervan zijn rechtsregels. Omdat normen vaak door de overheid opgelegd zijn, verschillen ze van staat tot staat. Normen worden opgevolgd door waarden. Waarden zijn idealen en motieven die het menselijke handelen bepalen. Waarden zijn soms maatschappelijk bepaald, en soms individueel, en zijn dus vaak subjectief.

Als laatste trede wordt intelligence in de zin van intelligentie genoemd. Intelligentie is de combinatie van de alle hiervoor genoemde fasen. Deze benadering van intelligence wijkt dus af van de politiële benadering (en de benadering die wij hanteren). De politiële benadering van intelligence zullen we nu kort toelichten.

Binnen de politie wordt intelligence voorgesteld als de trede na kennis en de laatste trede van de piramide. Intuïtie, normen en waarden vallen hiermee buiten het bereik van IGP. Om nu kennis daadwerkelijk geschikt te maken voor het nemen van beslissingen bijvoorbeeld in het kader van de opsporing en criminaliteitspreventie, is er nog een laatste stap nodig: kennis moet worden omgevormd tot intelligence. In het kader van criminaliteitsanalyse is intelligence het sluitstuk van een reeks analyses, het is een eindproduct. Binnen IGP is het de bron waarop beslissingen en handelingen worden afgestemd. In deze visie is intelligence de hoogste en meest vergaande vorm van kennisanalyse: het is bruikbare, specifieke kennis die kan worden ingezet bij het oplossen van bepaalde problemen (hier is de link met de probleemgestuurde politie gelegd, zie subsectie 5.1.2). De definitie van intelligence zoals gebruikt binnen IGP luidt '*information designed/interpreted for action*' (Minnebo 2004: 14). In deze praktische toepasbaarheid verschilt intelligence dus van kennis. Intelligence is het resultaat van geanalyseerde kennis. Hierbij is kennis dan informatie die van een context is voorzien en informatie is op zijn beurt data die een betekenis heeft gekregen (dit kan door interpretatie en integratie).

B: Tekortkoming van de piramidale visie

Wij hebben echter een bezwaar tegen de hierboven behandelde politiële product-definitie en zullen een andere, onzes inziens bredere definitie hanteren die meer recht doet aan de complexiteit van het concept. Ons bezwaar tegen deze productbenadering is niet zozeer dat de definitie onjuist is. Ons bezwaar zit in het feit dat een productbenadering niet goed duidelijk maakt wat intelligence voor de politie zo aantrekkelijk maakt. Het feit dat data wordt geïnterpreteerd, de hieruit voortkomende informatie in een context wordt geplaatst en vervolgens wordt gebruikt voor een actie, maakt het nog geen intelligence. Want wat is een actie? Beter is het te spreken van een beslissing. In dit opzicht zou de bovenstaande definitie van intelligence binnen IGP luiden 'geïnterpreteerde informatie gericht op het nemen van beslissingen'. Maar ook daarmee wordt volgens ons de toegevoegde waarde ten opzichte van andere informatie-modaliteiten niet gegeven.[220]

C: De door ons gehanteerde definitie

Op het moment dat iemand kennis neemt van informatie, wordt deze automatisch in een context geplaatst en geanalyseerd en dan wordt er onvermijdelijk een beslissing genomen op basis van die informatie (dat kan ook de beslissing zijn om geen actie te

[220] Wij merken hier op dat het een uitdaging is om intuïtie, normen en waarden te proberen te integreren in IGP. Volgens de benadering van Van de Herik kan er slechts dan uiteindelijk sprake zijn van een intelligente politie. IGP blijft in dit opzicht steken bij zijn vijfde element, te weten kennis.

ondernemen). Volgens ons moet intelligence dan ook niet primair worden gezien als een product, maar als een proces. Intelligence is een activiteit met geheel eigen kenmerken, en deze kenmerken maken het een voor de politie aantrekkelijk concept, maar zorgen ook voor uitdagingen (onder andere het uitvoeren van scenario-analyses). De door ons gehanteerde definitie van intelligence luidt dan ook: "(*Intelligence is) de overkoepelende term voor de reeks van activiteiten – van het vaststellen van een inlichtingenbehoefte en het verzamelen van informatie tot analyse en verspreiding – die in het geheim plaatsvinden en die zijn gericht op het bewaken of vergroten van veiligheid door middel van het geven van voorwaarschuwingen voor bedreigingen of potentiële bedreigingen op een manier die ruimte biedt voor een tijdige implementatie van een preventief beleid of strategie (…).*" (zie ook sectie 1.2, definitie één). De waarde van het concept voor de politiepraktijk ligt in de veronderstelde voorspellende waarde: dat is wat intelligence aantrekkelijk maakt voor de politie. Hier liggen echter belangrijke uitdagingen voor de politie. De twee belangrijkste uitdagingen die wij hier noemen zijn (a) het bereiken van een intelligente evaluatie van de kennisanalyse, en (b) het bepalen van de risico's die met het uitvoeren van de diverse acties gepaard gaan. De punten (a) en (b) kunnen samengevat worden als scenario-analyses. In de volgende sectie bekijken we hoe de Nederlandse politie in theorie probeert te komen tot IGP.

5.5 Twee uitwerkingen van IGP in Nederland

Voordat we IGP voor Nederland uitwerken, merken wij eerst op dat verschillen in nationale contexten maken dat in ieder land IGP anders wordt benaderd. In Groot-Brittannië was een belangrijker organisatorische herindeling van de instanties die zijn betrokken bij de bestrijding van georganiseerde criminaliteit een speerpunt van de IGP ontwikkeling. In de V.S. wordt IGP met name gezien als een *tool* in de strijd tegen terrorisme. Nederland heeft weer een geheel eigen context waarbinnen IGP zich afspeelt (zie verderop).

Voor de specifieke Nederlandse context merken wij voorts op dat de CIE in theorie een grote bijdrage kan leveren aan het succes van IGP: de CIE is het enige onderdeel van de politie dat met HUMINT mag werken en dat maakt de CIE-informatie van grote waarde voor IGP. Van oudsher hebben CIE-en echter een gesloten cultuur, hetgeen heeft geresulteerd in een terughoudende opstelling bij de ontwikkeling van IGP (zie Klerks 2010: 118). In hoofdstuk zeven zullen we analyseren in hoeverre IGP in de CIE-praktijk vorm krijgt. In deze sectie gaat het om de wijze waarop de Nederlandse politie in het algemeen probeert te komen tot IGP.

In de loop der jaren hebben verschillende organisatieonderdelen van de politie zich met de ontwikkeling en implementatie van IGP bemoeid. In deze sectie behandelen wij de belangrijkste ontwikkelingen van IGP, beginnende bij de eerste poging om tot een gestandaardiseerde uitwerking van het concept te komen, te weten ABRIO (5.5.1). Daarna komt het Nationaal Intelligence Model (NIM) (5.5.2) aan bod. Het NIM is bedoeld als de stuwende kracht achter IGP vandaag de dag (2011). We zijn ons ervan bewust dat elders binnen de politie belangrijke organisatieonderdelen en werkgroepen betrokken zijn bij (elementen van) IGP. Het is echter onmogelijk om deze allemaal in dit proefschrift te behandelen. Wij beperken ons tot de voornoemde twee.

5.5.1 ABRIO

IGP in Nederland wordt al sinds 2000 ontwikkeld. In 1999 stelden Meesters, Kortekaas en Tragter dat IGP pas kan worden geïmplementeerd als aan de volgende elementen is voldaan: (1) de eigen informatievoorziening is op orde (2) alle betrokken partijen managen hun kerncompetenties en hebben oog voor die van hun partners en (3) er moet op structurele basis sprake zijn van uitwisselen van gegevens, informatie en kennis tussen partijen. Kortom, er was voor de politie nog meer dan genoeg werk te doen voordat IGP geïmplementeerd kon worden. In 2000 kreeg het toenmalige programmabureau ABRIO de opdracht om IGP te ontwikkelen voor de Nederlandse politie.[221] ABRIO is destijds begonnen met de ontwikkeling van procesmodellen en gestandaardiseerde producten en heeft acht uitgangspunten benoemd waaraan voldaan moet worden om van IGP te kunnen spreken. Het gaat om (1) oriëntatie op de criminaliteitsproblemen en risico's in de samenleving, (2) organisatie van probleemverantwoordelijkheid, (3) sturen, afstemmen en monitoren (*plan-do-check-act*) op strategisch, tactisch en operationeel niveau binnen elk organisatorisch niveau, (4) besluitvorming vindt plaats op grond van analyseproducten, (5) toepassing van de 80-20 regel, oftewel het Pareto-principe[222], (6) er is een kwalitatief hoogwaardig informatie- en intelligence proces, (7) een goede informatievoorziening is gerealiseerd, en (8) opgedane kennis wordt structureel benut en geborgd (zie IOOV 2009: 19 e.v.). Feitelijk zijn de uitgangspunten de randvoorwaarden waaraan volgens ABRIO moet zijn voldaan voordat er van IGP gesproken kan worden.

De zienswijze van ABRIO en de acht uitgangspunten zijn echter volgens ons onduidelijk. Met name de door ABRIO gehanteerde begrippen en definities zijn onduidelijk. Zo is het niet duidelijk wat nu precies de criteria voor 'hoogwaardigheid' zijn, laat staan wat 'kwalitatief hoogwaardig' is. En wanneer kan er worden gesproken van een 'goede informatievoorziening'? Wat is het verschil tussen (a) een kwalitatief hoogwaardig informatie- en intelligenceproces en (b) een goede informatievoorziening? Bovendien, vloeit het laatste niet voort uit het eerste? Kortom, de uitgangspunten van ABRIO zijn misschien theoretisch een stap in de goede richting, maar bieden in de praktijk te weinig houvast voor de politie om daadwerkelijk IGP te implementeren.

ABRIO heeft het IGP-concept omgevormd in een aantal deelprojecten. Deze projecten dienden gestandaardiseerde producten op te leveren die ervoor moesten zorgen dat men overal eenzelfde ontwikkeling zou doormaken. ABRIO heeft de werkprocessen en producten die zouden moeten leiden tot IGP uitgebreid beschreven. Zo zijn er rapportages omtrent analyse, waarin definities worden gegeven van belangrijke termen (criminaliteitsanalyse, Criminaliteitsbeeld Analyse et cetera). Daarnaast wordt beschreven hoe om te gaan met restinformatie, hoe het *briefing*- en debriefing-proces eruit dient te zien en op welke wijze het sturingsmodel dient te werken. ABRIO heeft dus uitgebreid aandacht besteed aan alle onderwerpen die iets met IGP te maken hebben en deze gedetailleerd beschreven. De standaardisering van verschillende aspecten van het politiewerk die tot IGP behoren was een belangrijke focus van ABRIO.

---

[221] ABRIO is in 2006 opgehouden te bestaan. Delen van de werkgroep zijn doorgegaan onder VtSPN.

[222] Dit houdt in dat een gering aantal oorzaken (beperkte input of moeite) verantwoordelijk is voor het merendeel van de resultaten, oftewel: 80% van de omzet wordt bepaald door 20% van de producten. Dit principe houdt dus in dat een organisatie zich het beste kan richten op de 20% van de werkzaamheden die 80% van de opbrengsten opleveren.

Het streven naar standaardisering is aan de ene kant begrijpelijk. Immers, als alle korpsen de elementen van IGP anders interpreteren en toepassen, is er van één IGP geen sprake. Het probleem van ABRIO is echter dat het met name is gebleven bij product- en procesbeschrijvingen. Hoe het vervolgens moest worden geïmplementeerd, is een vraag waaraan ABRIO niet is toegekomen. Het beschrijven van het analyse-werkproces is één ding, het daadwerkelijk toegepast krijgen van de processen is heel iets anders. Hierover meer in hoofdstuk zeven.

Het ABRIO project is in 2006 door de Inspectie Openbare Orde en Veiligheid (IOOV) geëvalueerd. Volgens de IOOV bestaat er binnen de meeste korpsen draagvlak voor ABRIO–producten. Daarenboven is men binnen de politieorganisatie doorgaans positief over deze producten. De meeste ABRIO-producten zouden bovendien door de korpsen zijn geïmplementeerd, alhoewel er tussen de korpsen onderling verschillen zijn in de mate waarin de producten worden gebruikt (Beumer et al. 2006: 69 e.v.). Op deze plaats nemen wij een voorschot op het empirische hoofdstuk zeven. Wij hebben namelijk vrij weinig in de praktijk teruggezien van de ABRIO-producten. De producten waren wel binnen de door ons onderzochte korpsen bekend in de zin dat men wist waar ze gevonden konden worden. Vrijwel niemand heeft er inhoudelijk kennis van genomen. Eén CIE heeft er zelfs voor gekozen om de procesbeschrijving van de CIE te herschrijven omdat die van ABRIO te moeilijk zou zijn. Wellicht verschillen onze bevindingen van die van de IOOV omdat wij verschillende methoden van onderzoek hebben toegepast. Het IOOV heeft in haar onderzoek met name gebruik gemaakt van de methode van enquêtes: aan alle korpsen zijn vragenlijsten toegestuurd met onder andere vragen omtrent de implementatie van ABRIO. Wij hebben echter een etnografisch veldwerkonderzoek uitgevoerd waarbij wij participerende observatie en interviews als methode van dataverzameling hanteerden. Het IOOV heeft daarom wellicht een breder zicht op de implementatie, terwijl wij meer in de diepte hebben gekeken. Dat gezegd hebbende: wij constateren dat er op de werkvloer weinig wordt gedaan met de ABRIO-producten.

5.5.2 Het NIM

Inmiddels is de Nederlandse benadering van IGP vorm gegeven in het Nationaal Intelligence Model (NIM). Het NIM is de uitwerking van het concept IGP en wordt gezien als de standaard voor de Nederlandse politie. De Raad van Hoofdcommissarissen (RvHC) heeft het NIM in 2008 geaccordeerd en heeft ieder korps verplicht om vaart te maken met de implementatie van IGP en het NIM: in 2012 moeten alle korpsen volgens IGP werken (IOOV 2009). Hiermee wordt volgens de Politieacademie een einde gemaakt aan de vrijblijvendheid waarmee IGP tot dan toe is benaderd (Kop en Klerks 2009).

Het NIM wordt in het visiedocument “Tussen Wijk en Wereld” (NIM 2008; 2011) toegelicht. Het strategische speerpunt van het NIM is het landelijk invoeren van IGP ten behoeve van de effectiviteit van het politiewerk. Hiertoe geeft het NIM aan (1) op welke wijze de informatie de politie aanstuurt en (2) op welke wijze de politie op de informatieprocessen stuurt (Kop en Klerks 2009: 18). Zelf wordt het NIM door de strategische beleidsgroep intelligence als volgt geformuleerd: “*Het nationale intelligence model is het samenhangende stelsel van informatieknooppunten, stuurploegen en uitvoerende eenheden, functionerend binnen de kaders van het bevoegd gezag*” (NIM 2009: 7). Het gaat volgens deze beleidsgroep om een samenhangend stelsel ten behoeve van de sturing van het politiewerk.

In deze sectie behandelen wij de kernaspecten van de Nederlandse IGP volgens het NIM. Dit zijn (A) de drie criminaliteitsniveaus, (B) het stelsel van stuurploegen, weegploegen en informatieknooppunten, (C) ICT, (D) het delen van informatie en de politiecultuur, en (E) de rol van criminaliteitsanalyse en informatieknooppunten. Deze kernaspecten zullen in hoofdstuk zeven worden gebruikt voor verdere analyse aangaande de mate waarin het NIM is geïmplementeerd. Wij behandelen het NIM uitgebreid omdat het de belangrijkste Nederlandse invulling van IGP is.

A: De drie criminaliteitsniveaus

Het NIM maakt onderscheid in drie niveaus van criminaliteit die elk een eigen sturingsniveau kennen. Het eerste niveau wordt gevormd door de lokale criminaliteit en ordeverstoring op wijk- dan wel districtsniveau. Het tweede niveau is de criminaliteit of verstoring van de openbare orde die de districtsgrenzen overschrijdt. Het derde niveau is de zware georganiseerde criminaliteit of openbare orde-problematiek van nationaal of internationaal niveau.

Op elk van de drie niveaus moet volgens het NIM-concept een informatieknooppunt worden ingericht. Deze zijn weinig verrassend genaamd (1) lokaal informatieknooppunt (LIK), (2) regionaal informatieknooppunt (RIK) en (3) nationaal informatieknooppunt (NIK). In de praktijk spreekt men van het 'LIKRIKNIK-kanaal'. Deze informatieknooppunten leveren volgens het NIM gestandaardiseerde en 'stapelbare' informatieproducten op waarmee op het gehele politiewerk gestuurd kan worden.

Het idee is dus dat er een onderscheid te maken is in criminaliteitsniveaus. Dit onderscheid in criminaliteitsniveaus is op het conceptuele niveau van het NIM nog wel te maken. In de praktijk is het echter problematisch. Het probleem is dat criminaliteit wordt beoordeeld en bekeken aan de hand van kenmerken van de politieorganisatie zelf, te weten de indeling in verschillende regio's. Criminaliteit (waaronder terrorisme) wordt dan in een soort keurslijf gewrongen die geen recht doet aan de aard van criminaliteit zelf. Een crimineel of een terrorist is niet altijd bewust bezig met het acteren op een bepaald criminaliteitsniveau. Zo vindt de zwaarste vorm van georganiseerde criminaliteit (niveau 3) altijd plaats binnen een bepaalde regio. Een liquidatie is aan de ene kant een moord die in een specifieke regio plaatsvindt, maar waarvan de achtergronden op het niveau van de (inter)nationale georganiseerde criminaliteit spelen. En waar kunnen de huiskamerbijeenkomsten van potentiële terroristen onder worden geschaard wanneer de aanwezigen bewoners van dezelfde wijk zijn en naar dezelfde kerk of moskee gaan? Het NIM brengt dus een kunstmatig onderscheid aan tussen vormen van criminaliteit dat in de praktijk niet te maken is. Beroepscriminelen en potentiële terroristen trekken zich nu eenmaal weinig van regiogrenzen of landsgrenzen aan: die grenzen zijn een uitvinding van de overheid.

Omdat bepaalde vormen van criminaliteit zowel regionale, bovenregionale als nationale aspecten hebben, richten de rechercheafdelingen van de regionale politiekorpsen en de nationale recherche zich op dezelfde subjecten en groeperingen. Dit komt ook vanwege capaciteitsoverwegingen. Het is onmogelijk voor de nationale recherche om met de ongeveer 800 medewerkers alle (inter)nationaal opererende criminelen aan te pakken. Veel moet zij overlaten aan de regionale recherche-afdelingen die qua aantallen medewerkers weliswaar kleiner zijn, maar wier aandachtsgebied geografisch afgebakend en daarom overzichtelijker is. Overigens speelt bij de regionale aanpak van bepaalde vormen van georganiseerde criminaliteit

ook het probleem van de regio-overstijgende werkzaamheden van de criminelen. De onderverdeling van de criminaliteit in drie niveaus is te gemakkelijk en gaat voorbij aan de realiteit van criminaliteit, namelijk dat het een soort continuüm betreft in plaats van een fenomeen dat in duidelijk afgebakende grootheden kan worden onderverdeeld.

B: Stelsel van stuurploegen, weegploegen en IKP's

Sturing vindt plaats door de zogenoemde 'stuurploegen'. Elk criminaliteitsniveau kent zijn eigen stuurploeg. Stuurploegen stellen prioriteiten in zowel de aanpak van criminaliteit en overlast als de inzet van de politie. Zaken die door de stuurploeg worden behandeld, worden voorbereid door zogenoemde 'weegploegen'. Het NIM zegt over deze stuurploegen het volgende: **"***Er is landelijke sturing door afspraken over de aard, kwaliteit en tijdigheid van veiligheidsproducten. Op alle niveaus zijn er stuurploegen die sturen op basis van real time veiligheidsbeelden. De stuurploegen krijgen hun informatie van de informatieknooppunten. De medewerkers van de informatieknooppunten verzamelen, verwerken, analyseren en verstrekken stelselmatig informatie. Informatie over locaties, delicten en daders. En informatie over knooppunten van goederen-, mensen-, geld- en informatiestromen.*" (NIM 2009: II).

Een stuurploeg stuurt zowel op het informatieproces als op het tactische vervolg (bijvoorbeeld de opsporingsonderzoeken). Het informatieproces wordt gestuurd door middel van een intelligence-agenda die door de nationale stuurploeg wordt vastgesteld. Een intelligence-agenda is een overzicht van onderwerpen waar de nationale stuurploeg meer informatie over wenst om zo een effectieve en efficiënte sturing mogelijk te maken. Deze intelligence-agenda wordt op basis van het Nationaal Dreigingsbeeld (NDB) vastgesteld. Het NIK stelt de informatiestrategieën en inwinplannen op die verplicht worden uitgevoerd door de regionale korpsen. Het RIK kan vervolgens op haar beurt een regionaal inwinplan opstellen welke door een Districtelijk Informatie Knooppunt (DIK) moeten worden uitgevoerd. De informatieproducten die door een LIK worden gemaakt moeten antwoord geven op de vragen van een RIK, en de producten van een RIK moeten antwoord geven op de informatievragen van het NIK. Op deze manier worden de informatieprocessen op alle niveaus op elkaar afgestemd.

In een stuurploeg is zowel de politie als het OM en het openbaar bestuur vertegenwoordigd.[223] Dit maakt het mogelijk om de gehele politie te sturen, dus zowel de opsporing als de handhaving. Daarnaast is het volgens het NIM noodzakelijk om alle bij de sturing betrokken partijen bij elkaar te hebben omdat dan kan worden gekomen tot een integrale aanpak van bepaalde criminaliteitsproblemen. Georganiseerde criminaliteit kan dan zowel strafrechtelijk als bestuursrechtelijk (middels bijvoorbeeld de Wet bevordering integriteitsbeoordelingen door het openbaar bestuur, oftewel wet BIBOB)[224] worden bestreden (Kop en Klerks 2009:

[223] Volgens Van den Broek (2010: 39) is in 2010 door vertegenwoordigers van de politie en het OM afgesproken dat de intelligence-agenda door het OM en het bestuur worden vastgesteld. Wij zijn verder niet bekend met deze afspraak en gaan uit van de situatie dat de stuurploeg (waarin ook de politie zitting heeft) in gezamenlijkheid de intelligence-agenda vaststelt. De complexe relatie tussen de politie en het OM met betrekking tot IGP valt buiten de kaders van ons onderzoek. Wij zullen hier dan ook niet verder op ingaan.

[224] De Wet BIBOB biedt de mogelijkheid voor gemeentelijk, provinciaal en landelijke bestuursorganen om bepaalde vergunningsaanvragen te beoordelen op mogelijk misbruik voor criminele activiteiten. Zo kan op basis van deze wet een vergunning voor exploitatie van een horecagelegenheid worden

22; Van Daele et al. 2010). Het NIM ziet IGP als een concept dat toepasbaar is op de gehele politieorganisatie, en niet alleen de rechercheonderdelen die zijn belast met de opsporingstaak.

Stuurploegen werken onder het gezag van de driehoek, te weten de korpschef, korpsbeheerder en hoofdofficier van justitie.[225] Grofweg is de verdeling tussen de stuur- en weegploegen als volgt: de driehoek werkt op strategisch niveau (beleidsmatig), de stuurploeg op tactisch niveau (het voorbereiden van de opsporing en handhaving) en de weegploeg op tactisch en operationeel niveau (het uitvoeren van de opsporingsonderzoeken en handhaving) (Kop en Klerks 2009: 20).

Het is echter nog maar de vraag in hoeverre deze centrale aansturing van de politie een bijdrage levert aan een succesvolle bestrijding van de criminaliteit. Volgens het NIM werken de regionale korpsen immers volgens de intelligence-agenda die op landelijk niveau is vastgesteld. Maar hoeveel inzicht heeft de landelijke stuurploeg en het NIK op de lokale problematiek? En hoeveel ruimte heeft een regionaal korps om een eigen intelligence-agenda op te stellen voor de regionale problemen? Het NIM legt de uiteindelijke besluitvorming bij een landelijke stuurploeg, hetgeen een zeer verregaande centralisatie van de besluitvorming is. Maar wellicht anticiperen de opstellers van het NIM op de vorming van een nationale politie die in 2012 een feit moet zijn.[226]

Er wordt volgens het NIM overigens op alle aspecten van het politiewerk gestuurd: "*Elke eenheid begint met een korte briefing. Deze start met een overzicht van de hotspots en hotshots. Daarna worden de opdrachten van de dag uitgezet"* (NIM 2009: II). In Nederland probeert het politiemanagement de teugels steviger in handen te krijgen met behulp van deze methode van briefen/debriefen. Politiemensen worden dan met opdrachten gericht de straat op gestuurd (gebriefd) en moeten aan het einde van de dienst kunnen aantonen in hoeverre de opdracht is vervuld (gedebriefd) (ABRIO 2003). In hoeverre dit een succes is, kan nog niet gezegd worden. Wel wordt hieruit duidelijk dat IGP niet alleen bedoeld is om de politie efficiënter te maken, maar ook om het management een stevigere positie te geven (zie Vanlandschoot 2005: 129).[227]

C: ICT

Het NIM geeft ICT een belangrijke rol binnen IGP. Zo dient er sprake te zijn van *real time* informatie op basis waarvan een stuurploeg beslissingen neemt. Informatie die is verzameld door een rechercheur dient dus vrijwel direct beschikbaar te zijn voor het management en direct een rol te kunnen spelen bij besluitvorming. Het NIM (2009) stelt over ICT het volgende:

---

geweigerd indien een aanvrager van de vergunning bepaalde criminele antecedenten heeft. Het doel van de wet is om naast de strafrechtelijke aanpak van georganiseerde criminaliteit ook een bestuurlijke aanpak mogelijk te maken.

[225] Dit is de stuurploeg in de praktijk. Volgens de wet wordt het gezag gevormd door de burgemeester en de officier van justitie, artikel 12 jo. 13 Politiewet 1993.

[226] Zie de brief van de Minister van Veiligheid en Justitie aan de Tweede Kamer d.d. 14 december 2011 voor de plannen van het kabinet met betrekking tot de vorming van een nationale politie (*Kamerstukken II*, 2010/11, 29 628, nr. 231).

[227] Met name in de Nederlandse benadering van IGP ligt de nadruk op het verstevigen van het politiemanagement en leiderschap. In andere landen is dit minder het geval, hetgeen wellicht komt door een van nature sterkere politiehiërarchie dan in Nederland.

"Innovatieve ICT stelt de stuurploegen in staat verbanden te leggen en informatie in de context te interpreteren. Deze gevalideerde informatie wordt gepresenteerd op kaarten waarin informatie van politie, overheid en open bronnen samenkomt. De lokale, regionale enlandelijke veiligheidskaart zijn geheel ingeburgerde begrippen."

(…)

"Eenmaal op pad worden alle eenheden voorzien van de voor de opdracht benodigde informatie. Op het moment dat een eenheid het gebied inrijdt verschijnt alle informatie over dat gebied. Wanneer zij belast is met de controle van verkeersknooppunten dan is deze informatie bijvoorbeeld afkomstig uit de CatchKen.[228] *Wanneer ze belast is met observatie dan verschijnt op kaart niet alleen de vermoedelijke vastgestelde plaats van het subject, maar ook de posities van contacten, favoriete kroegen en parkeerplekken. Gedetailleerde kaarten van panden en straten zijn on-line beschikbaar."*

Innovatieve ICT speelt duidelijk een belangrijke rol bij IGP. Informatie afkomstig uit verschillende onderdelen van het politiebedrijf wordt gekoppeld en geografisch weergegeven. Sterker nog: het is de bedoeling dat de agent op straat direct (*real-time*) over deze informatie kan beschikken.

De vraag is echter of het NIM hier niet een te rooskleurig beeld schetst van de ICT-situatie bij de politie. Dat er in ieder geval nog bijzonder veel moet worden verbeterd aan de informatiehuishouding, blijkt wel uit de politiepraktijk. Uit rapporten van de Algemene Rekenkamer uit 2005 volgt dat er op het terrein van ICT-ontwikkelingen en standaardisatie binnen de Nederlandse korpsen nog veel gedaan moet worden. De Rekenkamer concludeerde destijds al dat "*kostenbeheersing voorop is komen te staan, ten koste van het tijdig realiseren van één informatiehuishouding voor de Nederlandse Politie*" (Algemene Rekenkamer 2005). In 2011 constateerde de Algemene Rekenkamer wederom dat er nog steeds grote problemen zijn met de ICT bij de politie (Algemene Rekenkamer 2011). Het gevolg van ICT-voorzieningen die niet goed op elkaar zijn afgestemd, is dat de gewenste koppeling van informatiedatabanken niet mogelijk is. Als ieder korps een eigen databank heeft, blijven er 25 informatie-eilandjes bestaan. Informatie van korps Haaglanden is dan bijvoorbeeld niet beschikbaar voor Amsterdam-Amstelland, hetgeen indruist tegen het principe van *need to share* (zie subsectie 5.4.4). Gebrekkige informatievoorziening zorgt voor een gebrekkig analyseproduct, hetgeen binnen IGP aan de basis van alle besluitvorming ligt. Het is dus essentieel dat er sprake is van uniforme ICT-voorzieningen. Zo maken de 26 korpsen gebruik van 850 verschillende applicaties die niet of slecht met elkaar kunnen communiceren. De RvHC heeft inmiddels besloten dat de Basis Voorziening Opsporing (BVO) de standaardapplicatie is voor het verwerken van opsporingsinformatie (Algemene Rekenkamer 2011: 75 e.v.). Hiermee probeert de raad te komen tot een vorm van standaardisatie. Het probleem van BVO is echter dat het draait op een sturingssysteem uit de jaren '80: het is verouderd en daarmee ook gebruikersonvriendelijk (Algemene Rekenkamer 2011: 78). Bij het streven naar

[228] *Catch Ken* is het geautomatiseerde controlesysteem dat de politie bij verkeerscontroles inzet. Nummerplaten worden automatisch gescand en kunnen worden vergeleken met een achterliggende database, onder andere om te beoordelen of er nog bekeuringen open staan, of de auto voorkomt in andere politiebestanden of, indien het breed wordt ingezet, om de bewegingen van de betreffende auto'(s) te monitoren.

uniformering is kennelijk genoegen genomen met een zeer verouderd computersysteem (zie De Koning 2010; Algemene Rekenkamer 2011). Inmiddels (2011) staat er een nieuw systeem klaar om geïmplementeerd te worden en BVO te vervangen: SUMMIT. Misschien dat dit systeem een verbetering van de informatiehuishouding zal opleveren. Of en in hoeverre dit het geval is, zal moeten blijken uit toekomstige audits van onder andere de Algemene Rekenkamer.

D: Delen van informatie en de politiecultuur

Naast de focus op sturing en ICT, richt het NIM zich ook op een (voorondersteld) cultuuraspect van de politie:

"Elke eenheid beschikt over de benodigde informatie. Need to share is onderdeel van de cultuur geworden. Wanneer een eenheid een kenteken van een auto controleert dan is meteen bekend welke teams ook op de bestuurder werken. De eenheid krijgt niet alleen informatie. Ook geeft zij voortdurend informatie terug. Informatie uit directe waarneming en over verdachte omstandigheden wordt actief gedeeld. Dit is mondelinge en beeldinformatie omdat alle voertuigen beschikken over foto- en videoapparatuur die voortdurend is verbonden met meldkamer en informatieknooppunt" (NIM 2009: II).

In het NIM wordt het belang van het delen van informatie onderstreept: alleen indien analisten beschikken over alle relevante informatie, kunnen zij een volledige en objectieve criminaliteitsanalyse maken. De enige die kan beoordelen of bepaalde informatie van belang is voor het goed vervullen van zijn taak is de analist zelf, dus het NIM gaat ervan uit dat informatie op voorhand gedeeld moet worden. Het idee is dat degene die de informatie als eerste heeft verzameld er op moet kunnen vertrouwen dat andere collega's correct met 'zijn' informatie om zullen gaan. Volgens het NIM gaat het hier dus om een cultuuromslag: informatie wordt niet langer informeel gedeeld, maar beweegt zich gericht en gestuurd via officiële wegen. Het delen van informatie is binnen het NIM een continue activiteit van de politiemedewerker geworden. Informatie stroomt vrijelijk tussen de verschillende politieonderdelen.

De achterliggende gedachte lijkt te zijn dat de huidige politiecultuur wordt gekenmerkt door een strikt doorgevoerd '*need to know*' denken. Het *need to know* is echter synoniem geworden met een bepaalde cultuur, te weten een cultuur waarbij geheimzinnigheid de boventoon voert. Op basis van het *need to know* denken zouden politiemensen onnodig informatie voor anderen achterhouden, mogelijk vanuit de gedachte 'kennis is macht' of vanuit –behartenswaardige- privacyoverwegingen.

Het eerste kenmerk van '*need to know*' is dat iemand over alleen die informatie beschikt die hij nodig heeft voor het vervullen van zijn taak (Colby 1976; CPRG 1997). Het tweede kenmerk van een *need to know* cultuur is het bestaan van *old boys networks*: officieuze netwerken van politiecollega's die buiten de officiële wegen onderling informatie uitwisselen.[229] Deze *old boys networks* hebben een aantal nadelen. Zo is het delen van informatie afhankelijk van de wil van de verstrekker van de informatie. Daarnaast houdt het nut van deze netwerken voor het delen van informatie op te bestaan op het moment dat de leden ervan niet langer binnen de

[229] Zoals wij nog in hoofdstuk zeven toelichten, zien wij de *old boys networks* als informele infrastructuren voor informatie-uitwisseling. Zie subsectie 7.6.2.

politie werkzaam zijn. Zij worden immers niet meer gevoed met politie-informatie. *Old boys networks* zijn dus onbetrouwbaar en niet-structureel. Of, en zo ja, wie er in de plaats treden van de uitgetreden leden hangt af van subjectieve factoren. De basis van deze netwerken is over het algemeen onderling vertrouwen. Het officieuze, informele karakter en de subjectiviteit van deze netwerken maken ze bijzonder lastig te sturen. Dit maakt *old boys networks* in strijd met de sturingsgedachte van IGP. Wij ontwaren een tweeledige doelstelling van het NIM indien het gaat om *need to share*: ten eerste moet de onnodige geheimhouding worden doorbroken en ten tweede moeten de informatie-uitwisseling die plaatsvindt via de *old boys networks,* worden geformaliseerd en geïnstitutionaliseerd. Het uitgangspunt binnen het NIM (en de politie in het algemeen) lijkt te zijn dat er sprake is van een cultuur van onterechte en onnodige geheimhouding. Geheimhouding door de politie is echter niet altijd onterecht en onnodig.

Geheimhouding binnen de opsporing kan legitieme redenen hebben. Zo worden bepaalde onderzoeken afgeschermd vanwege een mogelijk afbreukrisico: als degene tegen wie het onderzoek is gericht erachter komt dat hij in onderzoek is, dan kan dat mogelijk leiden tot maatregelen van zijn kant waardoor het onderzoek spaak loopt. Daarnaast moet de informatie die kan leiden tot het identificeren van informanten worden afgeschermd, ook voor medewerkers van de politie die met die informatie misschien betere analyses hadden kunnen maken. Het veiligheidsrisico voor de betreffende informant is eenvoudigweg te groot. Overigens moet bij het delen van politie-informatie ook rekening worden gehouden met relevante privacybepalingen, zoals de Wet Politiegegevens. Het is eenvoudigweg niet toegestaan om alle informatie organisatiebreed te delen, zeker niet daar waar het informatie uit het artikel 9, 10 of 12 domein betreft (zie sectie 4.4). Het is interessant om te bezien hoe de politie in de praktijk omgaat met de *need to share* gedachte in die gevallen waarbij geheimhouding eigenlijk geboden is. Hier gaan wij in hoofdstuk zeven dieper op in.

E: Criminaliteitsanalyse en de informatieknooppunten

Binnen het NIM is het analyseproces een onlosmakelijk onderdeel van het gehele opsporingsproces geworden en bedienen de leden van de stuurgroepen zich van geanalyseerde informatie bij het nemen van hun beslissingen. In het NIM (2008) staat het als volgt beschreven:

"De uitvoering van het rechercheproces is op een hoger niveau gebracht. De analyseomgeving is ingrijpend veranderd. En de rol van de analist ook. Rechercheurs en analisten beschikken op alle niveaus over gevalideerde instrumenten om informatie te analyseren: statistische technieken en geografische en dader-profiling maar ook forensic intelligence vormen standaards. Met kennis van zaken gebruiken rechercheurs instrumenten om scenario's te genereren en tegenspraak te organiseren. De analist is een volwaardige partner op sturingsniveau.

Medewerkers van informatieknooppunten zijn vakvolwassen. De vragen die zij uitzetten zijn niet alleen S.M.A.R.T. [230] *maar ook toegesneden op de rol van de collega. Alle collega's hebben hun eigen informatieprofiel: Zij zien wat ze nodig*

[230] SMART staat voor 'Specifiek, Meetbaar, Acceptabel, Realistisch en Tijdgebonden'. Door aan de SMART-criteria te voldoen voorkom je dat doelstelling vaag en vrijblijvend blijven.

hebben: niet minder, niet meer. De wijkagent krijgt de operationele informatie over zijn werk de districtschef zijn tactische sturingsinformatie en de korpschef haar strategische informatie"(NIM 2008: II)

Het NIM en ABRIO hebben veel aandacht besteed aan het uniformeren van analyseproducten. Deze producten staan in het 'productenboek' van ABRIO. Hierin staat bijvoorbeeld concreet omschreven waaruit een beschrijving van een Crimineel Samenwerkingsverband (CSV) minimaal dient te bestaan (leden, criminele activiteiten, samenwerkingsduur et cetera). De reden hiervoor is dat de verschillende korpsen vergelijkbare analyseproducten opleveren zodat het NIK deze analyses kan 'stapelen'. Het zou immers onwerkbaar worden voor het NIK als ieder korps een andere CSV-beschrijving hanteert.

Criminaliteitsanalyse vindt plaats op drie niveaus. Het eerste is het operationele niveau. Dit zijn analyses ten behoeve van de uitvoering van de opsporing. Voorbeelden hiervan zijn een analyse van een CSV, een bronanalyse van een informant en een dreigingsanalyse in een concreet geval. Operationele analyses zijn over het algemeen afgebakende analyses waarbij de nadruk met name ligt op het structureren van grote hoeveelheden informatie. De interpretatieve vragen die een operationeel analist stelt zijn bijvoorbeeld 'waarom belt crimineel A met crimineel B'? Vaak gaat het om schematische overzichten van criminele netwerken: wie heeft contact met wie, wie heeft welke rol in het netwerk et cetera.

Het tweede niveau is het tactische niveau. Tactische analyses zijn gericht op het formuleren van een specifieke aanpak en de inzet van beschikbare politiecapaciteit. Een voorbeeld van tactische analyses is het beschrijven van de verschillende CSV's die zich in een bepaald afgebakend gebied (crimineel, geografisch) manifesteren. Op basis van de tactische analyse moet worden besloten welk CSV op welke manier moet worden aangepakt. Dit vergt wat meer interpretatie van de kant van de analist. Zo moet hij proberen in te schatten hoe de netwerken functioneren en welke aanpak het gewenste resultaat zal opleveren. De analist moet dan zowel de netwerken in kaart brengen alsmede de verwachte interactie met de opsporing.

Het derde niveau is het strategische niveau. Strategische analyses zijn analyses op beleidsniveau. Een voorbeeld van een strategische analyse is een Criminaliteitsbeeld Analyse (CBA) of een Nationaal Dreigingsbeeld (NDB). De naam CBA zegt het eigenlijk al: de analist beschrijft daarin de verschillende aspecten van een crimineel fenomeen, zoals een drugsmarkt. Strategische analyses lijken in dit opzicht meer op sociaal wetenschappelijk onderzoek en vergen dus meer en andersoortige interpretatie dan operationele en tactische analyses. Vaak wordt voor de functie van strategisch analist een academicus aangetrokken. Met name de operationele en de tactische analyses worden al langer door de politie toegepast.

Volgens het NIM moet criminaliteitsanalyse een onderdeel worden van het gehele opsporingsproces. Criminaliteitsanalyse bestaat echter al langer dan IGP. In Nederland dook het voor het eerst op aan het einde van de jaren '80. Het werd met name gebruikt voor analyses van georganiseerde criminaliteit. Gedurende de jaren '90 werd criminaliteitsanalyse verder ontwikkeld, maar toch bleef het van ondergeschikt belang binnen het opsporingsproces. Dit blijkt overigens ook in Groot-Brittannië, waar analyse gedurende een lange tijd werd gezien als een vrouwenbaan en iets dat niet echt tot het politiewerk behoorde (Cope 2004). IGP probeert hier verandering in te brengen. Criminaliteitsanalyse is eigenlijk het primaire inhoudelijke werkproces geworden. De analist is degene die de inzichten moet genereren op basis

waarvan beslissingen genomen kunnen worden. Rechercheurs zijn primair belast met het verzamelen van informatie: de interpretatie dient overgelaten te worden aan analisten.

De bovenstaande ontwikkeling is niet zonder kritiek gebleven. Fijnaut stelde in een interview met het NRC-Handelsblad (Meeus en Verlaan 2010) dat er bij de recherche zich een 'klein drama' zou afspelen. IGP leidt er volgens hem toe dat rechercheurs met jarenlange ervaring bij de relatief onervaren analist langs moeten voor informatie. "*De wereld op zijn kop*", aldus Fijnaut (Meeus en Verlaan 2010). Daarnaast is het nog steeds de vraag of analisten binnen de politieorganisatie echt geaccepteerd gaan worden. Criminaliteitsanalyse is in veel gevallen bureauwerk dat ver af staat van de dagelijkse werkzaamheden van een rechercheur. Dit geldt met name voor de strategische analyses. Het is dan ook niet voor niets dat Ratcliffe (2008) in zijn IGP model veel aandacht besteedt aan de beïnvloeding van de beleidsmakers door analisten. Ook voor de beleidsmakers zijn analisten een beetje een vreemde eend in de bijt. Het is daarom geenszins vanzelfsprekend dat analisten een invloedrijke positie binnen het politiebedrijf zullen innemen. Meer hierover in hoofdstuk zeven.

Tot slot

Het NIM is een concept dat nog geïmplementeerd dient te worden. Inmiddels is er een programma intelligence in het leven geroepen met als taak het implementeren van het NIM en het ondersteunen van de korpsen daarbij. Het programma richt zich primair op het verbeteren van de samenhang en afstemming tussen de informatieknooppunten op landelijk en regionaal niveau (Kop en Klerks 20092009: 19). Om het NIM nader te concretiseren, is er een architectuur ontwikkeld waarin de richting en inrichting van de informatieorganisatie worden beschreven. Daarnaast voorziet deze architectuur in een eenduidige terminologie die de samenhang dient te versterken.

Met het NIM en het programma intelligence is het concept van IGP voor de Nederlandse politie uitgewerkt. Inmiddels is (enigszins) duidelijk *wat* de politie verstaat onder IGP. De echte uitdaging zit daarom zoals gezegd in *hoe* het in de praktijk wordt toegepast. Deze hoe-vraag is het onderwerp van hoofdstuk zeven.

5.6 Nieuwe begrippen en nieuwe analyses

De vraag die nu rijst is in hoeverre IGP en het NIM overeenkomsten vertonen met het politieke inlichtingenwerk. Wij hebben in hoofdstuk twee de HP-kenmerken van de veiligheidsdiensten beschreven. Het gaat om de bescherming van de nationale veiligheid (HP-kenmerk 1), het geven van voorwaarschuwingen (HP-kenmerk 2), de intelligence cyclus (HP-kenmerk 3) en de geheimhouding (HP-kenmerk 4). Dit zijn vier elementen die terugkomen in onze definitie van intelligence (zie hoofdstuk sectie 1.2). In deze sectie bekijken wij in hoeverre deze elementen terugkomen in het NIM. Wij zien met name de voorwaarschuwing (5.6.1) en de intelligence cyclus (5.6.2) terug in het NIM. De geheimhouding is echter iets waar het NIM vergeleken met de veiligheidsdiensten een hele andere benadering heeft (5.6.3). De bescherming van de nationale veiligheid wordt in het geheel niet door het NIM behandeld. Dit kenmerk laten wij dan ook buiten beschouwing.

5.6.1 HP-kenmerk 2: voorwaarschuwing

Een traditionele politie doet aan waarheidsvinding en is reactief. Er wordt gekeken naar wat er is gebeurd. Een veiligheidsdienst zorgt voor tijdige waarschuwingen en kijkt dus naar wat er mogelijk nog staat te gebeuren. IGP en het NIM hebben ook de ambitie om voorwaarschuwingen te geven. Het NIM verwoordt dit als volgt:

"Door de dreigingskaarten verdwijnt de algemene surveillance. Blauw is op de plek waar de (verwachte) dreiging het grootst is of waar vanuit handhavingoogpunt politietoezicht gewenst is. Op de rustige plekken is de wijkagent met de ogen en de oren open nog steeds zichtbaar aanwezig: niet voor de opvolging maar om de kennis van de samenleving actief levend te houden" (NIM 2008: II).

De veiligheidsdiensten hebben zich gespecialiseerd in de 'kunst' van het (geïnformeerd) gissen (Johnston 2005; Gill en Phythian 2006). Absolute zekerheid is voor veiligheidsdiensten niet nodig, daarvoor zijn de in het geding zijnde belangen veel te groot. Dit is bij de opsporing van strafbare feiten door de politie anders. Vanwege de mogelijke inzet van executieve bevoegdheden vereist wetgeving een hoge mate van waarschijnlijkheid: de rechter dient in het Nederlandse negatief wettelijke bewijsrecht immers overtuigd te worden van de schuld van de verdachte alvorens hij tot een eventuele veroordeling kan overgaan.

IGP kan, wanneer succesvol geïmplementeerd, tot gevolg hebben dat de politie zich primair richt op intelligence, met de daarbij behorende waarschijnlijkheidsindicatie. Vanwege IGP ontwikkelt de criminaliteitsanalyse zich vanuit een historische omschrijving van criminele fenomenen naar een voorspellende variant. De lector intelligence van de politieacademie verwoordde het als volgt: "*Voor een succesvolle intelligencegestuurde organisatie zijn juist ook het uitvoeren van verklarende analyses naar de oorzaken van een probleem, prescriptieve analyses naar mogelijke maatregelen voor het probleem, evaluerende analyses naar de effecten van de maatregelen en voorspellende analyses over de toekomst van grote toegevoegde waarde*" (Den Hengst-Bruggeling 2010). Onder de noemer IGP ontwikkelt de Nederlandse politie zich dus steeds meer naar een model met mogelijk een voorspellende waarde. De gewenste toename in effectiviteit en efficiëntie wordt met name bereikt door niet langer alleen maar te doen aan opsporing van strafbare feiten, maar ook door criminaliteit te gaan bestrijden. Bestrijden omvat concepten als tegenhouden en verstoren. Bij tegenhouden wordt er een beschrijving gemaakt van criminele processen en wordt er (in theorie) zo vroeg mogelijk in het proces een barrière opgeworpen. Dit hoeft dus niet te bestaan uit opsporingsonderzoeken.

Een ander uitgangspunt van IGP dat van belang is, is het streven naar zogenoemde 'informatie maximalisatie'. Hierbij gaat het niet alleen om informatie uit de politieorganisatie, maar ook om informatie uit openbare bronnen (Jansen 2001: 13). De politieorganisatie is in deze benadering net een stofzuiger die overal informatie opzuigt om die te analyseren en te verwerken tot intelligence (zie De Hert en Vis 2005). Deze informatiezucht is vergelijkbaar met die van de politieke inlichtingendiensten (zie hoofdstuk twee): pas wanneer de beschikking is over alle mogelijke informatie, bestaat er de mogelijkheid om alle potentiële toekomstige bedreigingen te onderkennen. Net als bij veiligheidsdiensten is de informatiebehoefte van de politie die werkt volgens IGP in principe onverzadigbaar. Meer informatie is beter politiewerk, is de gedachte. Dit heeft echter implicaties voor bijvoorbeeld de privacy in een samenleving. Het streven van de politie naar meer informatie zal altijd

op gespannen voet staan met het uitgangspunt van privacy, namelijk dat de staat pas een inbreuk maakt op de vrijheidsrechten van burgers als zij hiervoor een concrete aanleiding heeft. Een ander probleem speelt bij de efficiency en effectiviteit van de politie zelf. De vraag is namelijk of het streven naar zoveel mogelijk informatie echt goed is. Meer informatie zal niet automatisch leiden tot een betere informatiepositie, maar kan juist leiden tot een overvloed aan informatie en overbelasting van de analisten (Sheptycki 2004). *Dataoverload* is een serieus probleem voor veiligheidsdiensten en inmiddels ook voor de politie, maar nog niet iets waar echt een oplossing voor is gevonden.

Waarschijnlijk is deze voorspellende waarde één van de belangrijkste redenen waarom IGP zo populair is binnen de politie. Het is echter beter om te spreken van 'vermeende voorspellende waarde'. De vraag is namelijk in hoeverre politieorganisaties in staat zullen zijn om daadwerkelijk zinnige uitspraken te doen over de mogelijke trends en ontwikkelingen van criminaliteit. Voor de veiligheidsdiensten creëert deze zweem van voorspellend vermogen over het algemeen verwachtingen die zij niet kunnen inlossen: het is volgens sommigen de reden waarom ze gedoemd zijn om te falen (Turner 2004).

5.6.2 HP-kenmerk 3: de intelligence-cyclus

De traditionele politie werkt volgens het werkproces van het opsporingsonderzoek (zie sectie 2.11). Het uitgangspunt van het opsporingsonderzoek is het verzamelen van bewijs. Het verzamelen van informatie geschiedt dus met een specifiek doel: het bewijzen van een interpretatie van de strafrechtelijk relevante waarheid. Dit maakt de politie tot een reactieve organisatie. Een veiligheidsdienst gaat echter uit van de intelligence-cyclus en heeft het opbouwen en in stand houden van een informatiepositie als zelfstandige doelstelling. Deze diensten werken proactief in de zin dat zij zelfstandig op zoek gaan naar informatie en niet afwachten totdat informatie bij hen terecht komt. IGP, en meer specifiek het NIM, is een verschuiving van het politiewerk van opsporingsonderzoeken naar de intelligence-cyclus (zie ook: Den Hengst-Bruggeling 2010: 17). Het opbouwen en in standhouden van de informatiepositie is met het NIM een zelfstandige doelstelling geworden. Het gaat niet meer primair om het verzamelen van bewijs, maar om het beantwoorden van vragen die in de intelligence-agenda worden gesteld. Met andere woorden: sturen met en op informatie. Dit behoeft nadere uitleg.

De intelligence-cyclus hebben wij beschreven in een 8-stappen model (zie sectie 2.6). Het is een vraaggestuurd model dat aanvangt met een intelligence-behoefte van een consument (stap 1) welke leidt tot concrete vragen aan de inlichtingengemeenschap (stap 2). Vervolgens wordt er gericht informatie verzameld (stap 3) die wordt verwerkt (stap 4) en vervolgens wordt geanalyseerd (stap 5). Na de analyse volgt de productie en verspreiding van intelligence-producten (stap 6), hetgeen leidt tot maken en/of aanpassen van beleid (stap 7). Dit beleid heeft invloed op de context van de inlichtingengemeenschap en diens klanten/consumenten (stap 8), hetgeen leidt tot een nieuwe of aangepaste intelligence-behoefte. Als we vervolgens kijken naar het NIM, dan zien we de intelligencecyclus in grote lijnen terug.

Allereerst zijn IGP en de uitwerking daarvan in het NIM een vraaggestuurd intelligence-model. Dit is de eerste fase van de intelligencecyclus. Er wordt gestuurd met en op informatie. De stuurgroepen zijn de beleidsmakers, degenen die de informatievragen stellen aan de politie. Zij bepalen waar de politie zich de komende periode op gaat richten. Dit doen zij aan de ene kant door een intelligence-agenda op

te stellen en aan de andere kant door specifiek te kiezen voor een bepaalde aanpak van criminaliteitsfenomenen, de tweede fase van de cyclus. De intelligence-agenda is een soort inwinplan voor de politiekorpsen. De korpsen moeten de vragen uit de intelligence-agenda zoveel mogelijk beantwoorden, hetgeen betekent dat er gericht informatie moet worden verzameld. Dit is fase drie. Voor de verwerking van de ingewonnen informatie gaat het NIM uit van ICT-voorzieningen, fase vier. Eén van de belangrijkste elementen voor de politie vormt de vijfde fase, de fase van analyse. Er wordt in het NIM veel nadruk gelegd op verschillende vormen van analyse. De analyseproducten (zoals dreigingsanalyses, CBA's, CSV-omschrijvingen en geografische analyses) worden verspreid onder de stuurploegen op alle drie de niveaus (operationeel, tactisch, en strategisch), hetgeen de zesde fase van de intelligence-cyclus is. De stuurploegen maken op basis van de analyseproducten op de drie niveaus beleid, dit is fase zeven. De keuzes die vervolgens worden gemaakt voor een specifieke aanpak hebben een impact op de omgeving van de politie en de stuurploegen: bepaalde CSV's worden aangepakt door middel van opsporingsonderzoeken en verdwijnen mogelijk deels uit het criminele milieu, criminele processen raken verstoord et cetera. Dit heeft invloed op het criminele milieu en zal er bijvoorbeeld toe leiden dat criminele organisaties zich noodgedwongen aanpassen. Deze impact op de omgeving is de achtste fase. Een nieuwe omgeving leidt tot nieuwe informatievragen en de noodzaak tot nieuwe strategieën van de kant van politie en justitie. Hiermee is de cyclus rond.

Uit het bovenstaande volgt dat IGP en het NIM uitgaan van het proces van de intelligence-cyclus. In dit opzicht lijkt het werkproces van de intelligencegestuurde politie veel op het werkproces van de veiligheidsdienst. Naast het werkproces lijkt ook de doelstelling van IGP op die van de veiligheidsdiensten: het doel is immers het anticiperen op criminaliteit (en terrorisme) door het geven van voorwaarschuwingen. Er is echter ook een belangrijk verschil tussen IGP en het concept van intelligence. IGP gaat namelijk uit van een verregaande mate van transparantie en het delen van informatie, terwijl bij intelligence het uitgangspunt doorgaans geheimhouding is. Wij behandelen in deze subsectie tot slot deze het verschil van transparantie versus geheimhouding (subsectie 5.6.3).

5.6.3 HP-kenmerk 4: geheimhouding

Een traditionele politieorganisatie is zoveel mogelijk transparant, maar kent intern ook vaak verregaande geheimhouding (zie sectie 2.12). Een burgerlijke veiligheidsdienst kent zowel een verregaande interne als externe geheimhouding. IGP en het NIM hebben ingrijpende gevolgen voor de interne en externe geheimhouding van de politie. Allereerst behandelen we de externe geheimhouding.

De vraag die rijst is wie de politie controleert bij het bestrijden (en dus voorkomen) van criminaliteit. Dit is niet noodzakelijkerwijs de strafrechter. In bepaalde gevallen zullen bestuursrechters of civiele rechters het politieoptreden beoordelen, maar dit is doorgaans vaak afhankelijk van het initiatief van een benadeelde partij. Het is echter denkbaar dat het politieoptreden niet bekend wordt bij degenen die er door worden benadeeld. Een voorbeeld is de bestrijding van *cybercrime*, oftewel misdrijven die plaatsvinden op of met behulp van computers en het internet. Het internet is in veel opzichten ook voor het strafrecht en de politie onontgonnen terrein. Zo is het denkbaar dat de politie criminele netwerken op het internet (bijvoorbeeld zogenoemde *botnets*) alleen maar in kaart kan brengen door

software te installeren op de geïnfecteerde computers van gebruikers wereldwijd.[231] De meeste van die gebruikers zijn niet crimineel, maar slachtoffers van hackers. Als de politie ervoor kiest om zo'n netwerk te ontmantelen zonder dat er verdachten worden vervolgd, bijvoorbeeld omdat deze in landen verblijven waarmee Nederland geen uitleveringsverdrag heeft, dan komt er geen rechter aan te pas die beoordeelt of het optreden van de politie rechtmatig is geweest. Hoever de bestrijding van criminaliteit precies gaat en welke methoden en technieken worden ingezet, verdient onderzocht te worden. Dit valt evenwel buiten ons onderzoek. Belangrijk voor ons onderzoek is met name de interne geheimhouding en de ontwikkeling naar *need to share*.

Het uitgangspunt van *need to share* staat in eerste opzicht haaks op het onderdeel 'geheimhouding' in de definitie van intelligence. Binnen het NIM is delen echter de regel, geheimhouding de uitzondering. Volgens sommigen was dit hard nodig. Zij stellen dan ook dat "*intelligence needs to be reclaimed from the secret world, made less threatening to communities and used in their service"* (Griever 2004 in Ratcliffe 2008: 7). Dit heeft voor de verhouding tussen de veiligheidsdiensten en de politie mogelijk belangrijke gevolgen. Veiligheidsdiensten gaan namelijk wel uit van *need to know*. De vraag is hoe deze diensten kijken naar een politiedienst waar dit beginsel overboord is gezet. Is de politie nog wel te vertrouwen met gevoelige informatie? Leidt dit tot negatieve beeldvorming en zo ja, heeft dit gevolgen voor de samenwerking tussen de diensten? Een andere vraag is hoe de politiemensen zelf reageren op het nieuwe '*need to share*'. Ook voor hen is dit nieuw, en hoe zij erop reageren is nog maar de vraag.

5.7 Hoofdstukconclusie en antwoord op OV 2

In dit hoofdstuk hebben wij antwoord gegeven op OV 2: *Wat is het concept IGP en hoe beoogt dit concept de traditionele Nederlandse CIE te veranderen?* Wij hebben onder andere de achtergronden en uitgangspunten van het concept behandeld, en zijn uitgebreid op de Nederlandse invulling van IGP ingegaan.

IGP is één van de belangrijkste nieuwe ontwikkelingen in het moderne politiebestel. Het gaat uit van het adagium kennis is macht. IGP is het antwoord van de politie op de schaalvergroting waarmee in toenemende mate is geconfronteerd. IGP wordt binnen de politie over het algemeen gezien als een sturingsconcept waarbij (1) criminaliteitsanalyse leidt tot de opbouw en instandhouding van een informatiepositie welke (2) de besluitvorming faciliteert en waarbij (3) informatie zoveel mogelijk wordt gedeeld, dit alles ten behoeve (4) een proactieve en preventieve aanpak van criminaliteit en terrorisme. Criminaliteitsanalyse vormt in dit opzicht het hart (of beter: het brein) van het concept. Het biedt zoveel mogelijk een objectieve basis voor het nemen van beslissingen. IGP is een cyclisch proces, hetgeen betekent dat uit de analyse nieuwe informatievragen voortvloeien, die vervolgens het proces van informatie verzamelen sturen. Er wordt dus gestuurd met en op informatie.

Wij concluderen dat IGP geen oude wijn in nieuwe zakken is. De schaal waarop IGP geïmplementeerd wordt, maakt het uniek. Het is niet alleen het idee dat besluitvorming zoveel mogelijk gebaseerd moet zijn op objectieve feiten wat IGP nieuw maakt, maar zeker ook de omvang waarmee een standaardisering en

[231] Het KLPD heeft deze methode recentelijk toegepast op het zogenoemde Bredolab netwerk. Zie voor een analyse over de rechtmatigheid van dit concrete overheidsoptreden: Koning 2011.

uniformering van het politiewerk wordt beoogd is vernieuwend te noemen. IGP is een herziening van het gehele politiebestel: het verandert de wijze waarop de politie te werk gaat. Met andere woorden: het is een verschuiving van het politieparadigma. Van een reactieve, incidentgestuurde organisatie moet de politie intelligencegestuurd en proactief gaan werken.

Wanneer de Nederlandse uitwerking en invulling van IGP (het NIM) wordt bekeken, blijkt al snel dat de ambities groot zijn. Het vereist een complete herstructurering van de politie, en de vraag is in hoeverre de politiepraktijk in staat zal blijken om het NIM volledig te omarmen en implementeren. Is Nederland wel helemaal klaar voor een juiste implementatie van het concept? In hoofdstuk zeven gaan wij aan de hand van ons empirisch onderzoek in op OV 3: in hoeverre wordt IGP in de praktijk toegepast?

Niettegenstaande het feit dat de politie een enorme opgave heeft aan het implementeren van haar eigen veelomvattende benadering van IGP in de politiepraktijk, concluderen wij dat de politiebenadering (kort gezegd de beoogde objectivering van de besluitvorming binnen het politiewerk) volgens ons van een te beperkte zienswijze op IGP getuigt. Het concept beoogt immers tegemoet te komen aan de eisen die vandaag de dag aan de moderne politie worden gesteld: de criminaliteit en de bijbehorende risico's moeten efficiënt en effectief worden bestreden. In de veiligheidscultuur betekent dit dat de politie proactief dient te zijn en dat hierbij preventie van criminaliteit het uitgangspunt is. Proactiviteit en preventie vormen volgens ons de echte kern van IGP. De manier waarop de politie dat probeert te bereiken, is door middel van het implementeren van het concept van intelligence. Wij hebben IGP dan ook gedefinieerd als 'de implementatie van het concept van intelligence in de context van de bestrijding van georganiseerde criminaliteit en terrorisme'. Het doel van intelligence is voorts het geven van voorwaarschuwingen zodat preventieve maatregelen kunnen worden genomen.

In hoofdstuk twee hebben wij de kenmerken van de hoge politie beschreven, en in dit hoofdstuk hebben we bekeken in hoeverre deze elementen terug te vinden zijn in het concept IGP. Een intelligencegestuurde politie kent sterke overeenkomsten met een hoge politie. Allereerst zijn de proactieve werkwijze en de preventieve doelstelling ook sterk aanwezig bij IGP. Waar ze van elkaar verschillen is dat IGP zich niet richt op de bescherming van de nationale veiligheid, en de hoge politie wel. Maar uiteindelijk gaat het wel allebei om het bereiken van een vorm van veiligheid. De wijze waarop IGP vorm geeft aan de veiligheid toont weer bijzonder veel gelijkenis met de wijze waarop de veiligheidsdiensten dat doen: het gaat bij IGP in de kern om het voorkomen van risico's. In dit opzicht past IGP naadloos in de veiligheidscultuur van vandaag de dag. Het voorkomen van risico's vereist het opbouwen en in stand houden van een informatiepositie, wederom een essentieel kenmerk van IGP. Daarnaast is het ook een HP-kenmerk (2). De politie bereikt dit met name door criminaliteitsanalyse een belangrijke rol in het gehele politieproces te geven. Maar ook andere elementen van de intelligence-cyclus worden door IGP binnen de context van het politiewerk gebracht (HP-kenmerk 3). Waar IGP en politieke intelligence in eerste opzicht van elkaar lijken te verschillen, is geheimhouding (HP-kenmerk 4). IGP probeert aan geheimhouding een einde te maken. Dit betreft echter met name de interne geheimhouding. Er is weinig dat wijst op een vermindering van de externe geheimhouding. Het valt overigens nog te bezien in hoeverre IGP leidt tot een vermindering of vermeerdering van externe geheimhouding: dit ligt echter buiten de scope van ons onderzoek.

Met de implementatie van IGP lijkt er weinig verschil meer te zijn tussen veiligheidsdienst en de politie. IGP verkleint in theorie de scheiding tussen de beide organisaties. Om echt te kunnen beoordelen in hoeverre IGP leidt tot een vermenging van de veiligheidsdiensten met de politie, zal moeten worden bekeken in hoeverre er sprake is van een daadwerkelijke implementatie van intelligence in de politiepraktijk. Dat gebeurt in hoofdstuk zeven.

6| Het praktijkonderzoek

Dit hoofdstuk behandelt het praktijkonderzoek. Het geeft inzicht in hoe we het onderzoek hebben opgezet (sectie 6.1), hoe de data in de praktijk zijn verzameld (sectie 6.2) en hoe deze data vervolgens zijn geanalyseerd (sectie 6.3). Daarnaast geven wij ook meer inzicht in de persoonlijke ervaringen die voor dit onderzoek van belang zijn geweest (sectie 6.4). Immers, bij een etnografisch onderzoek is de onderzoeker het belangrijkste meetinstrument: hij neemt bepaalde gebeurtenissen waar, selecteert welke gebeurtenissen relevant zijn voor het beantwoorden van de probleemstelling en de onderzoeksvragen, schrijft deze gebeurtenissen op en gaat over tot een analyse van het verzamelde materiaal. Het is onmogelijk om alle gebeurtenissen, indrukken en keuzemomenten die een rol hebben gespeeld tijdens het veldwerk in dit hoofdstuk te behandelen. Het doel van dit hoofdstuk is duidelijk te maken hoe wij te werk zijn gegaan en op welke wijze de volgende empirische hoofdstukken tot stand zijn gekomen. Wij sluiten dit hoofdstuk af met de beantwoording van de vraag hoe wij met het gevaar van '*going native*' zijn omgegaan (sectie 6.5).

6.1 Opzet van het onderzoek

Ons onderzoek is exploratief van aard. Dat ligt voor de hand, want er is nog weinig empirisch onderzoek naar IGP en wij willen een beeld verkrijgen van (1) de praktijk van IGP en (2) de wijze waarop de praktijk de verhouding tussen de veiligheidsdiensten en de politie, meer specifiek de AIVD en de CIE beïnvloedt. Onze aanpak is als volgt. Eerst hebben we de beschikbare literatuur over IGP, inlichtingen- en veiligheidsdiensten, intelligence en de politieorganisatie bestudeerd. Daarnaast hebben we ons ook in diverse juridische aspecten van het onderwerp verdiept. Dit heeft geleid tot het formuleren van de centrale probleemstelling en de onderzoeksvragen. Tijdens de literatuurstudie hebben we een aantal organisaties geïdentificeerd die in aanmerking komen voor een onderzoeksstage. Uiteindelijk bleef de politieorganisatie als enige relevante onderzoeksgroep over. We hebben ook onderzoek gedaan bij het CBP, maar met het schrappen van een onderzoeksvraag gericht op privacyvraagstukken binnen de politie, is deze stage minder relevant geworden voor dit onderzoek. Deze stage heeft overigens wel deels input geleverd voor een deel van hoofdstuk vier, met name daar waar het de WPG betreft.

Na de literatuurstudie (inclusief de juridische aspecten) kwam de fase van het praktijkonderzoek. We hebben de politie benaderd en hebben daar vervolgens bij twee afdelingen, te weten de RIO en de CIE, ongeveer 2,5 jaar stage gelopen. In het eerste anderhalf jaar hebben we drie tot vier dagen per week stage gelopen. De overige dagen hebben we gebruikt voor het analyseren van de data en het schrijven van onderdelen van het proefschrift. Het volgende halve jaar lag de nadruk meer op het verwerken en analyseren van de data en het schrijven. Toen hebben we voor het laatste jaar de verhouding stageplek/universiteit omgedraaid en waren we twee dagen op de stageplek en de overige drie op de universiteit.

In 2009 hebben we besloten om ons te beperken tot de CIE en de RIO: deze organisatieonderdelen wijken in verregaande mate af van de tactische opsporingsteams. De CIE heeft vanwege haar specifieke juridische taakstelling een bijzondere informatiepositie: het is de enige politiedienst die met informanten mag werken. In de afscherming van de informanten ligt ook de kern voor de cultuur van

geheimhouding. De term 'inlichtingeneenheid' geeft het eigenlijk al aan: de CIE is primair een organisatie waar geheimhouding een essentiële rol speelt. Dit staat haaks op bepaalde uitgangspunten van IGP, zoals het *need to share*-streven. Voorts leidt de geheimhouding tot een grotendeels van de buitenwereld afgeschermde wereld. Voor een onderzoeker is het interessant om te bezien hoe een voorgenomen veranderingsproces zoals de implementatie van IGP in de praktijk daadwerkelijk in die wereld uitwerkt. De vraag is bijvoorbeeld in hoeverre de historisch verankerde cultuurkenmerken leiden tot verzet tegen IGP. De RIO is daarentegen een nieuw organisatieonderdeel dat specifiek is gericht op de implementatie van IGP. De RIO's worden de laatste jaren van de grond af opgebouwd en hebben nog geen historisch verankerde cultuur. De RIO's zijn eigenlijk de belichaming van IGP, en het is dan ook interessant om te beoordelen hoe het concept binnen dit jonge organisatieonderdeel uitwerkt. En vanzelfsprekend zijn er ook andere organisatieonderdelen waar IGP wordt geïmplementeerd die het onderzoeken waard zijn. Echter, als we ook de tactische opsporingsteams en andere bijzondere afdelingen van de politie hadden onderzocht, dan zou het onderzoek veel te breed zijn geworden. We hebben ons dan ook beperkt tot de CIE en de RIO.

We hebben van tevoren besproken dat, naast (1) de literatuurstudie, (2) de participerende observatie en (3) de interviews de belangrijkste methoden van dataverzameling zouden zijn. Tijdens de onderzoeksstage hebben we een journaal bijgehouden voor het optekenen van de observaties. Bovendien werden we door een medewerker van de politieorganisatie begeleid bij de dagelijkse activiteiten van het onderzoek.

6.2 Dataverzameling in de praktijk

In deze sectie behandelen wij de drie methoden van dataverzameling waarvan we gebruik hebben gemaakt, te weten het literatuuronderzoek (subsectie 6.2.1), de participerende observatie (subsectie 6.2.2), de interviews (subsectie 6.2.3) en het literatuuronderzoek met betrekking tot de grijze literatuur die binnen de politieorganisatie aanwezig was (subsectie 6.2.4).

6.2.1 Het literatuuronderzoek

Een eerste belangrijke bron voor het onderzoek zijn de diverse publicaties over (1) het onderwerp IGP en (2) de door ons onderzochte organisaties, te weten de AIVD, CIE en de RIO. In de verkennende fase hebben wij de literatuur over IGP bestudeerd en de schaarse literatuur over de verhouding tussen de AIVD en de politie. De resultaten van het literatuuronderzoek zijn te vinden in hoofdstukken twee tot en met vijf en vormen de basis voor de lijst van onderwerpen die tijdens het onderzoek naar voren kwamen. Hoe meer het onderzoek vorderde, des te meer specifieke literatuur wij konden gebruiken. In een latere fase kwam daar de literatuur bij die theoretische inzichten bood, bijvoorbeeld de theorie van Russel Hardin (2005) met betrekking tot vertrouwen (zie subsectie 8.3.2)

6.2.2 De participerende observatie

Het eerste onderdeel van onze dataverzameling bestond uit participerende observaties. Bij deze vorm van dataverzameling wordt directe waarneming van relevante data mogelijk doordat de onderzoeker deelneemt aan het sociale leven van de betrokkenen

(Boeije 2006: 272-274). In deze subsectie behandelen we de twee belangrijkste aspecten van onze participerende observaties, te weten (A) de periode van observaties en de onderzoeksgroep, (B) de registratie van de observaties. Vier relevante vragen bij B zijn (1) hoe hebben wij dit gedaan? (2) in welke mate waren de betrokkenen op de hoogte van het feit dat wij hen observeerden? (3) wat hebben we opgeschreven? En (4) wat voor zover relevant hebben we niet opgeschreven?

A: Periode en onderzoeksgroep

Wij hebben twee jaar lang participerende observaties gedaan. Voor het grootste deel (anderhalf jaar) hebben wij dit bij een RIO verricht en een half jaar bij een CIE. Tijdens deze periode zijn wij betrokken geweest bij diverse projecten, werkgroepen en andere interne en externe samenwerkingsverbanden die soms van korte duur (vier weken) en soms van langere duur (één jaar) waren. Daarnaast hebben we mogen participeren in twee omvangrijke politiële onderzoeken: (1) een aan terrorisme gerelateerd onderzoek en (2) een onderzoek naar een crimineel netwerk. Onze werkzaamheden in het kader van deze projecten betrof aan de ene kant advisering op juridisch en criminologisch gebied, aan de andere kant werden wij ingezet voor diverse vormen van informatieverzameling en verwerking (zoals het maken van presentaties, selecteren van relevante literatuur op diverse onderwerpen *et cetera*). In ruil voor deze activiteiten werd het ons toegestaan om aantekeningen te maken en data te verzamelen voor het onderhavige onderzoek. Wij kunnen in verband met de overeengekomen geheimhouding voor de meeste werkgroepen en activiteiten waarin wij een rol hebben gespeeld niet precies aangeven wat het onderwerp was. Wij volstaan met de vaststelling dat het allemaal onderwerpen waren die gerelateerd zijn aan de implementatie van intelligence in de praktijk van de CIE.

B: De registratie van de observaties

De registratie van de observaties vond plaats via een dagboek, zowel schriftelijk als digitaal. We hebben altijd duidelijk te kennen gegeven dat we onderzoek verrichtten en dat we daarom alles opschreven. De medewerkers van de afdelingen waar wij onderzoek deden waren hiervan op de hoogte, hetgeen niet wegneemt dat in de loop van de tijd deze bewustwording bij hen steeds minder werd. Dit had ook te maken met het feit dat we in toenemende mate betrokken werden bij de dagelijkse werkzaamheden van de politieorganisatie, waardoor men ons waarschijnlijk meer zag als collega dan als onderzoeker. Wij hebben een strikt onderscheid gehanteerd tussen werkzaamheden die wij voor de politie verrichtten, en onderzoeksactiviteiten. De eerste werden niet direct gebruikt voor onderzoek en vastlegging. Wanneer wij evenwel in aanraking kwamen met voor het onderzoek relevante informatie, noteerden we dat in een apart deel van het dagboek. Hiervoor introduceerden wij de door de CIE gehanteerde term ‘sturingsinformatie’ voor overige onderzoeksactiviteiten. Zo gebruikten wij deze informatie wel tijdens interviews en kwamen wij er in andere situaties, waarbij het duidelijk was dat wij bezig waren met het onderzoek, nog op terug. Dit laat onverlet dat de relevante informatie uiteindelijk niet is gebruikt, omdat bepaalde operationele belangen van de politieorganisatie zich daartegen verzetten.

6.2.3 De interviews

Naast de participerende observaties vormen de interviews met de medewerkers uit de praktijk de belangrijkste bron van informatie. In deze subsectie behandelen wij (A) de respondenten en (B) de opzet en uitvoering van de interviews.

A: De respondenten

Wij hebben in totaal 40 medewerkers geïnterviewd, van wie het grootste deel werkzaam was bij de CIE (21) en een groot deel bij de RIO (10). We hebben echter ook met enkele (voormalige) medewerkers van de AIVD gesproken. Met name voor de laatste categorie medewerkers geldt dat extra afscherming is geboden. Daarom zullen wij deze respondenten aanduiden met (voormalig) medewerker van de AIVD. Voor de medewerkers van de politie kunnen wij wel een aanduiding van hun rol geven. We hebben de volgende 40 functies geïnterviewd (vermeld in chronologische volgorde).

1. Maart 2007: Runner CIE (A)
2. Mei 2007: Hoofd CIE (A)
3. Mei 2007: Analist CIE (A)
4. Mei 2007: Analist CIE (B)
5. Juli 2007: Analist RIO (A)
6. December 2007: Teamleider tactiek (A)
7. Januari 2008: (Voormalig) medewerker AIVD (A)
8. Januari 2008: (Voormalig) medewerker AIVD (B)
9. Januari 2008: Teamleider RIO (A)
10. Februari 2008: (Voormalig) medewerker AIVD (C)
11. Februari 2008: Projectmedewerker IGP (A)
12. Oktober 2008: Teamleider CIE (A)
13. Oktober 2009: Runner CIE (B)
14. Oktober 2009: Hoofd CIE (B)
15. Februari 2009: Teamleider RIO (B)
16. Februari 2009: Teamleider CIE (B)
17. Maart 2009: Projectmedewerker IGP (B)
18. Maart 2009: Projectmedewerker IGP (C)
19. Maart 2009: Analist CIE (C)
20. Maart 2009: Analist CIE (D)
21. Maart 2009: Analist CIE (E)
22. Maart 2009: Analist RIO (B)
23. Maart 2009: Analist RIO (C)
24. Maart 2009: Teamleider CIE (C)
25. Maart 2009: Runner CIE (C)
26. Maart 2009: Analist RIO (D)
27. April 2009: Plaatsvervangend hoofd CIE
28. April 2009: Teamleider RIO (C)
29. April 2009: Hoofd CIE (C)
30. April 2009: Hoofd CIE (D)
31. April 2009: Analist CIE (F)
32. Mei 2009: Teamleider RIO (D)
33. Mei 2009: Teamleider tactiek (B)

34. Juni 2009: (Voormalig) medewerker AIVD (D)
35. November 2009: Teamleider CIE (D)
36. Mei 2010: Recherchekundige RIO (A)
37. November 2010: Teamleider CIE (E)
38. Maart 2011: Recherchekundige RIO (B)
39. Maart 2011: Runner CIE (D)
40. Maart 2011: Analist CIE (G)

In de bovenstaande lijst wordt duidelijk dat we gesproken hebben met 21 medewerkers van de CIE en tien van de RIO. Daarnaast hebben we vier (voormalig) medewerkers van de AIVD, drie medewerkers van een implementatieproject voor IGP en twee teamleiders van tactische opsporingsteams geïnterviewd. De reikwijdte loopt van medewerkers op de werkvloer tot de leidinggevenden. De interviews zijn daarnaast onderverdeeld in drie rondes.

In de periode maart tot en met juli 2007 hebben wij vijf verkennende interviews afgenomen die als doel hadden om bekend te worden met de afdelingen waar wij ons onderzoek hebben verricht. In dezelfde periode hebben we veel verkennende gesprekken gevoerd met verschillende medewerkers (ongeveer 50), welke tot doel hadden om ons bekend met de organisatie in het algemeen te maken. Omdat we deze gesprekken redelijk vrij wilden houden zonder de gesprekspartners direct in een interviewsetting te spreken, rekenen we deze gesprekken niet tot de interviews. Ze zijn grotendeels wel opgenomen in ons journaal, en een aantal van de gesprekspartners hebben we op een later moment alsnog geïnterviewd.

Een tweede ronde interviews (zes in totaal) hebben wij in de periode december 2007 tot en met februari 2008 gedaan. We waren beter bekend met de organisatie en waren in contact gekomen met een aantal medewerkers die relevante inzichten hadden met betrekking tot ons onderzoek. In de periode tussen de interviews lag de nadruk met name op participerende observatie en korte, ongestructureerde gesprekken die wij niet tot de interviews rekenen.

De meeste interviews (22) vonden in de derde ronde plaats die liep van februari tot juni 2009. Bij deze interviews hebben wij hulp gehad van een stagiaire, Ellen Bijl, die in totaal 19 mensen heeft geïnterviewd. Hiervan zijn twaalf interviews uiteindelijk gebruikt voor onze analyse. De overige zeven interviews hebben we niet kunnen gebruiken of hebben we in een later stadium over moeten doen. De reden lag in het feit dat een aantal respondenten achteraf heeft aangegeven dat ze liever direct met ons wilden praten in plaats van met een student en dat ze tijdens het interview niet alles hebben verteld wat ze ons wel zouden vertellen. Deze interviews hebben we zelf alsnog overgedaan.

Een vierde en laatste periode van interviews vond in 2010 en in 2011 plaats (vijf in totaal). Deze interviews hadden als doel om te peilen in hoeverre de bevindingen nog golden en of er relevante nieuwe ontwikkelingen hebben plaatsgevonden die een nieuwe ronde interviews noodzakelijk maakten. Dit is niet het geval gebleken. Sterker nog, bepaalde bevindingen uit de eerdere interviews en observaties bleken nog sterker te gelden tijdens deze latere interviews. Een voorbeeld hiervan is de wijze waarop de politie met de zij-instromers en andere medewerkers met een academische achtergrond is omgegaan. Enkele respondenten gaven in 2008 en 2009 aan dat academici niet goed werden opgevangen, en dat dit mogelijk zou kunnen leiden tot uitstroom van hoger opgeleid personeel. In 2010 en 2011 stelden respondenten dat bij veel van de onderzochte politieonderdelen er een behoorlijke

uitstroom was van dit hoger opgeleide personeel, waarmee de bewering uit 2008 en 2009 nog steeds actueel bleek.

Naast de interviews hebben we overigens ook veel korte gesprekken gevoerd van minder dan een anderhalf uur. Deze hebben we echter niet aangemerkt als interviews, maar meer als verkennende gesprekken (waaronder de eerder genoemde 50 uit 2007). Van een aantal mensen met wie we zo'n verkennend gesprek hebben gevoerd, hebben we op een later moment een interview afgenomen.

B: Opzet en uitvoering van de interviews

Tijdens de eerste verkennende gesprekken (die we niet hebben opgenomen in de interviews) bleek dat een vrije setting tot de beste resultaten leidde. De recherche is een informele organisatie waar een grote nadruk ligt op informele gesprekken. Wanneer er iets besproken moet worden, verkiest men het liefst de informele setting van de koffietafel of een kleinschalig overleg boven de formele vergadering, en dat gaat gepaard met aanzienlijke hoeveelheden koffie.[232] "*Even een bakkie koffie doen*" is dan ook een veelgehoorde aankondiging van overleg. Daarnaast wilden we voorkomen om middels de vraagstelling al teveel te sturen: omdat ons onderzoek exploratief is, wilden we dat de respondenten zelf elementen benoemden die zij relevant achtten voor ons onderzoek. We gebruikten weliswaar een lijst van onderwerpen die aan bod moesten komen, maar de interviews waren zo opgezet dat het meer het karakter had van een informeel gesprek. Het waren dus semi-gestructureerde interviews. De interviews duurden gemiddeld anderhalf uur. Een deel van de interviews is opgenomen met een taperecorder, en een deel is handmatig verwerkt.

De onderwerpen die in de interviews aan bod dienden te komen, zijn geselecteerd op basis van het verkennend literatuuronderzoek en de eerste verkennende gesprekken. Het ging in eerste instantie om de volgende zes onderwerpen: (1) IGP en intelligence, (2) sturing van het politiewerk, (3) proactiviteit en voorwaarschuwingen, (4) analyse, (5) de informatiehuishouding en (6) de relatie met de AIVD. De contouren van IGP in de praktijk en de relatie met de AIVD werden echter steeds duidelijker, wat leidde tot nieuwe onderwerpen. Dit bracht ons er in 2009 toe om de onderwerpen (7) 'geheimhouding' en het gerelateerde *need to share* toe te voegen. Vervolgens hebben we een aantal respondenten benaderd die ons hierover het één en ander konden vertellen. Een andere aanvulling had betrekking op het tweede onderwerp uit de lijst van onderwerpen (de sturing van het politiewerk). Uit de eerste interviews en onze observaties bleek dat (8) leiderschap een essentiële rol speelde. Dit onderwerp hebben wij tijdens het literatuuronderzoek bewust niet opgenomen in de lijst van onderwerpen die tijdens de interviews aan bod zouden moeten komen, omdat het voor ons niet duidelijk genoeg was. Wat verstaat men immers onder 'leiderschap'? Dit onderwerp bleek tijdens het onderzoek echter bijzonder relevant en kwam een aantal keren terug tijdens de interviews. Wij hebben dit in de laatste rondes (eind 2010 en 2011) opgenomen in de onderwerpenlijst.

We begonnen ieder interview met een korte introductie van het onderzoek en vroegen de respondent om kort iets over zijn geschiedenis bij de politie of de AIVD te

[232] Onderzoekers bij de politie betalen een prijs: onze inname van koffie nam in de eerste twee maanden toe van een (toch aanzienlijk) gemiddelde van vijf koppen per dag op de universiteit tot twaalf tot vijftien koppen bij de politie. Dat kan niet goed zijn voor de gezondheid. Toen wij de inname-frequentie trachtten te compenseren door over te stappen op thee, merkte één van de politiemannen op "een kopje gay voor meneer".

vertellen. De eerste vraag die we vervolgens stelden was "*ben je bekend met het concept IGP?*" (onderwerp één) en van daaruit volgde het verdere gesprek. Doorgaans kwamen de meeste IGP-gerelateerde onderwerpen na de eerste vraag aan bod. De overige onderwerpen (twee tot en met acht) lagen kennelijk minder voor de hand voor de respondenten, en deze hebben we gedurende het interview ingebracht. Overigens was de helft van de respondenten (20) niet in staat om op basis van eigen ervaringen verder in te gaan op de vraag naar de relatie tussen de politie en de AIVD. Uiteindelijk hebben wij met 20 respondenten gesproken die hier iets over konden vertellen.

Aan het begin van de interviews hebben we altijd duidelijk aangegeven dat het ging om een interview en dat we het wilden gebruiken in een openbare academische publicatie. De respondenten kregen anonimiteit toegezegd. Met de respondenten is daarnaast afgesproken dat ze het interviewverslag na het interview ter controle toegestuurd kregen, en met een aantal (met name de medewerkers van de CIE) is vervolgens afgesproken dat ze de relevante passages in dit boek waarin hun citaten zijn opgenomen konden beoordelen. Mochten ze, om wat voor een reden dan ook, bezwaar maken tegen de opname van een specifiek citaat, dan zouden wij deze verwijderen. Wij hebben onze taak dienovereenkomstig uitgevoerd. Er is geen gebruik gemaakt van ons verwijder-aanbod.

Naarmate het onderzoek vorderde, werden de interviews steeds 'dieper' van aard. In het begin ging het zoals gezegd om verkennende interviews en ging het over vrij algemene zaken, zoals de organisatie van de afdelingen waar wij onderzoek hebben gedaan. Later konden wij veel dieper in gaan op diverse onderwerpen, zoals de WPG en het streven om te komen tot *need to share*. Op deze manier hebben wij getracht een methodologisch probleem te ondervangen. Omdat dit onderzoek bijna longitudinaal van aard is, moet er periodiek een correctie van het onderzoek plaatsvinden betreffende de tijd (wij onderzoeken geen ontwikkeling, maar verrichten een exploratief onderzoek). Interviews uit 2007 zijn immers niet één op één te vergelijken met interviews uit 2011. Er kunnen inmiddels veranderingen hebben plaatsgevonden die van invloed zijn op de interviews. Wij hebben op twee manieren geprobeerd om dit methodologische probleem op te vangen. Ten eerste hebben we, zoals we hiervoor al hebben aangegeven, de interviews aangepast en steeds verder gestructureerd. De interviews die wij in de derde en vierde ronde hebben afgenomen, zijn dan ook veel dieper van aard. Ten tweede hebben we met de respondenten periodiek nog informele gesprekken gehouden waarin we hebben vastgesteld in hoeverre de meningen waren veranderd of bijgesteld. Zonder uitzondering gaven de respondenten aan dat er in vier jaar tijd nauwelijks veranderingen zijn opgetreden (behoudens de gebruikelijke veranderingen, zoals verhuizingen en personele ontwikkelingen die eigenlijk geen invloed hebben op de onderzoeksresultaten). Een in 2010 geïnterviewde recherchekundige verwoordde het als volgt: "(er is) *niks veranderd. We kabbelen gewoon wat door*." (sociaal gesprek recherchekundige, juni 2011). Een andere respondent gaf aan "*het lijkt wel alsof de tijd hier stil staat, dezelfde discussies blijven terugkomen*" (sociaal gesprek hoofd CIE, december 2010).

6.2.4 De ('grijze') literatuur

Een bijzondere bron van literatuur is de grijze literatuur. Dit is literatuur die doorgaans alleen binnen de politieorganisatie beschikbaar is, en niet daarbuiten. Het is voor andere onderzoekers die geen toegang hebben tot de politieorganisatie erg moeilijk om van deze literatuur gebruik te maken. Wij hebben de grijze literatuur

omwille van de afbakening van ons onderzoek en de openbaarmaking van resultaten slechts gebruikt als sturingsinformatie bij het afnemen van de interviews en het selecteren van locaties voor observaties. In dit opzicht hebben wij de grijze literatuur op dezelfde manier behandeld als de observaties. Zo hebben wij verschillende beleidsstukken met betrekking tot de samenwerking tussen de AIVD en de politie in kunnen zien, maar daar mogen we niet naar verwijzen. De relevante bevindingen uit die beleidsstukken hebben wij omgevormd tot specifieke vragen aan de respondenten, en op die manier hebben we geprobeerd om deze bevindingen toch te kunnen gebruiken. Een andere categorie van grijze literatuur zijn de afstudeerscripties van studenten aan de politieacademie. In veel gevallen worden deze scripties niet gepubliceerd, omdat ze betrekking hebben op onderwerpen die intern gevoelig liggen, zoals evaluaties van opsporingsonderzoeken en werkwijzen. In het kader van onze stage hebben wij wel toegang gekregen tot een aantal van deze scripties. Ook voor deze grijze literatuur geldt dat wij het alleen hebben gebruikt als sturingsinformatie.

6.3 De analyse van de data

Bij de analyse zijn we uitgegaan van datatriangulatie: wij hebben alleen informatie gebruikt die door twee andere, onafhankelijke bronnen is bevestigd. Dit is gedaan om te voorkomen dat onze bevindingen zijn gestoeld op anekdotes (overigens iets waar etnografisch onderzoek zich nooit helemaal aan kan onttrekken, vooral wanneer het wordt vergeleken met natuurwetenschappen). Voorts hebben we er naar gestreefd om zoveel mogelijk informatie uit verschillende methoden van dataverzameling te gebruiken. In veel gevallen hebben wij zowel observaties als interviewverslagen als ook (grijze) documenten die een bepaalde bevinding ondersteunen, gebruikt. De observaties hebben wij gedurende het onderzoek doorlopend geanalyseerd en gebruikt voor het opstellen van nieuwe interviewvragen in een latere fase en het verrichten van andere onderzoeksactiviteiten. Observaties zijn in mindere mate gebruikt in de empirische hoofdstukken, omdat het in bepaalde gevallen moeilijk is om te beoordelen of de observaties die zijn verricht in een operationele context binnen de geheimhoudingsverklaring vallen. Indien we die letterlijk zouden opschrijven, dan zou dat problemen kunnen opleveren met de afdelingen waar wij onderzoek hebben gedaan. Deze observaties zijn wel gebruikt voor de analyse en het beoordelen van theoretische modellen, maar wij gebruiken met name de citaten uit interviews ter illustratie van onze bevindingen.

Van alle interviews en observaties hebben wij een taxonomie gemaakt met alle relevante onderwerpen met betrekking tot de probleemstelling en de onderzoeksvragen. Aan de hand van deze classificatie hebben we de onderwerpen geselecteerd die inzicht geven in (a) de mate waarin IGP in de praktijk van het CIE-werk wordt geïmplementeerd en (b) de verhouding tussen de AIVD en de CIE/RIO. Deze onderwerpen hebben we uitgewerkt in praktijkbevindingen.[233] Vervolgens zijn we op zoek gegaan naar theoretische inzichten die een verklaring bieden voor datgene wat wij in de praktijk hebben gesignaleerd. Er bleken behoorlijk veel theoretische concepten te zijn die (onderdelen van) onze bevindingen mogelijk verklaren. Wij hebben de meest relevante concepten gebruikt en andere terzijde gelegd. Deze inductieve benadering ligt bij een exploratief onderzoek als dat van ons voor de hand, omdat het van tevoren bijna onmogelijk is om theorieën te selecteren. We hebben de

[233] Wij pretenderen overigens niet om wetmatigheden te formuleren die in alle gevallen geldig zijn. Vanwege de complexiteit van de sociale werkelijkheid en de mogelijke variabelen die een rol spelen bij een fenomeen als de verhouding tussen de AIVD en de CIE/RIO is dit onmogelijk.

analyse van de data overigens doorlopend gedaan, omdat we de interviews en de onderwerpen die we wilden observeren periodiek wilden aanpassen

Uit de 40 interviews, 200 informele gesprekken en overige observaties hebben wij moeten selecteren welke informatie we wilden gebruiken bij de schriftelijke presentatie van het empirische materiaal. Zoals we reeds eerder hebben vermeld, hebben we met name gebruik gemaakt van de interviews. De keuze voor specifieke citaten is in bepaalde gevallen (enigszins) arbitrair. Zo vertellen veel respondenten over de 'waan-van-de-dag-organisatie' die de politie is. Wij hebben hieruit de opmerkingen gekozen die volgens ons het meest in de buurt komen van de door ons geformuleerde praktijkinzichten.

6.4. Afspraken en geheimhouding

In deze sectie behandelen we de gemaakte stageafspraken met betrekking tot ons onderzoek. Bij binnenkomst hebben wij een geheimhoudingsovereenkomst getekend waarin wij hebben aangegeven dat we (1) geen operationele gegevens of andere gegevens zouden publiceren of anderszins openbaar maken en dat (2) de organisatie van tevoren kennis zou nemen van de inhoud van onze studie om te beoordelen of wij ons aan de overeenkomst hebben gehouden. Indien een publicatie van onze studie zou leiden tot verregaande negatieve gevolgen voor de organisatie, dan zou de organisatie het recht hebben de publicatie zes maanden tegen te houden. Uiteindelijk zou des studie wel worden gepubliceerd. We merken expliciet op dat op geen enkele manier invloed is uitgeoefend door de politieorganisatie om de inhoud van deze studie aan te passen of op een andere manier 'censuur' te plegen. Alle overwegingen over welke onderwerpen wij wel en welke wij niet hebben opgenomen in de uiteindelijke publicatie en de wijze van presentatie, komen volledig voor onze rekening.

6.5 Het veldwerk

In deze sectie behandelen we de praktijk van ons veldwerkonderzoek. Een onderzoeker die etnografisch onderzoek verricht selecteert en interpreteert de relevante data terwijl hij probeert zoveel mogelijk te ervaren wat zijn onderzoekssubjecten ervaren. Dit maakt de subjectieve beleving van de onderzoeker van groot belang bij de interpretatie van de data. Deze sectie geeft inzicht in hoe wij het onderzoek in de praktijk hebben ervaren en waar wij als onderzoekers mee te maken hebben gekregen. We beginnen bij de eerste indrukken die wij van de stageplek hadden (subsectie 6.5.1). Vervolgens behandelen wij de mate waarin we door de medewerkers van de stageplek werden geaccepteerd (subsectie 6.5.2). Daarna beschrijven wij de dynamiek van de politieorganisatie (subsectie 6.5.3). Wij besluiten de sectie en het hoofdstuk met het grote gevaar van etnografisch onderzoek waarbij de participerende observatie centraal staat: het risico van *going native* (subsectie 6.5.4). Deze sectie is verder in de ik-vorm geschreven: het is immers de weerslag van persoonlijke onderzoekservaringen.

Tot slot merken wij op dat wij niet aan de zogenoemde '*thick description*' doen die in veel etnografisch onderzoek gebruikelijk is. *Thick despription* is de wijze van verslaglegging die in de antropologie wordt gebruikt om de complexe en vaak subjectieve belevingswereld van de onderzoekssubjecten zo waarheidsgetrouw mogelijk weer te geven. Symbolen en andere cultuurgerelateerde uitingen worden uitgebreid en in detail beschreven, waarbij moet worden opgemerkt dat het welhaast onmogelijk is voor een antropoloog om daadwerkelijk datgene te ervaren wat zijn

onderzoekssubjecten ervaren (zie Geertz 1973; Peacock 2004: 104; Kempny en Burszta 2005: 95-96). Dit heeft met name een pragmatische reden: een dergelijke beschrijving draagt het gevaar in zich dat teveel zaken die onder de geheimhoudingsverplichting vallen worden openbaard. Dit zou problemen kunnen opleveren met de stageorganisatie wanneer wij het onderzoek willen publiceren. Om hieraan te ontkomen, hebben wij besloten om geen *thick description* te geven. Wij merken hierover expliciet op dat er op geen enkele wijze censuur door de stageorganisatie is uitgeoefend. In tegendeel: we hebben alleen maar medewerking gekregen. Het ontwijken van *thick descriptions* is onze eigen overweging geweest.

6.5.1 De eerste indruk: demystificatie van een instituut[234]

In maart 2007 begon de onderzoeksstage. Ik had me in die periode goed voorbereid door veel literatuur te lezen over de politie in het algemeen en intelligence in het bijzonder, en had daarom een beeld van de organisatie gekregen. De recherche is toch een instituut waarvan de innerlijke werking voor de meeste mensen verborgen zal blijven. Omdat ik niet kon weten hoe de organisatie precies zou werken en wat ik zou aantreffen, had ik van tevoren slechts wat verwachtingen en vage veronderstellingen. Ik verwachtte in eerste instantie aan de ene kant een dynamische werkplek, en aan de andere kant was ik me bewust van de problemen die de politie had met bijvoorbeeld de ICT-voorzieningen. Van collega's op de universiteit had ik eveneens een bepaald beeld gekregen van de organisatie. Zij bereidden me voor op enigszins norse mensen die eigenlijk niet zoveel op hebben met wetenschappelijke onderzoekers. Sommigen trokken ook het niveau van de politie naar beneden. Eerlijk gezegd zag ik het vooraf niet zo zitten om daar zes maanden door te brengen. Ik ging dus enigszins met lood in mijn schoenen naar de stageplek, me afvragend of ik er niet beter aan had gedaan om het te houden bij literatuuronderzoek en interviews. Daarnaast vond ik het eigenlijk ook wel spannend en was ik erg nieuwsgierig naar de mogelijke resultaten voor het onderzoek. Met mijn promotores en toenmalige dagelijks begeleiders had ik doorgesproken wat de beste manier zou zijn om de organisatie binnen te komen, en we besloten dat een bescheiden en afwachtende houding het beste zou zijn. Ik wilde niet overkomen als een arrogante academicus die de politiemensen de les komt lezen of die komt kijken wat ze allemaal fout doen. Dit is namelijk het beeld dat veel politiemensen van wetenschappelijke onderzoekers hebben. Ik nam mij voor om de eerste weken bij zoveel mogelijk mensen langs te gaan om uit te leggen wat ik kwam doen.

Nadat ik eerst een uur bij de ingang had moeten wachten omdat degene met wie ik een afspraak had zijn trouwdag was vergeten en dus niet op het werk was, werd ik door zijn secretaresse meegenomen naar de afdeling. Het gebouw waar de eenheid in 2007 was gevestigd, is vrij groot. Het heeft vier verdiepingen en veel vleugels waar verschillende eenheden waren gevestigd. Ik moest naar de derde verdieping. Het eerste wat opviel, was de grote hoeveelheid beveiligde deuren. Alle medewerkers hebben een persoonlijk intern legitimatiebewijs (een pas) waaraan een aantal autorisaties voor ruimten is verbonden. Wij moesten door vijf beveiligde deuren voordat we bij de afdeling waren. Op weg naar de afdeling moesten we door een lange, smalle en donkere hal met aan weerszijden ruimten die oorspronkelijk vrij grote, open ruimten moeten zijn geweest, maar waar door middel van kasten van

[234] De typering 'demystificatie van een instituut' hebben wij van één van de respondenten die onze verbazing omtrent de praktijk van het politiële inlichtingenwerk op deze wijze zeer treffend formuleerde.

diverse hoogten afscheidingen waren aangebracht. De grote ruimten werden op die manier opgedeeld in vele kleinere waar zich diverse eenheden en afdelingen van de recherche bevonden. Op de lagere kasten stonden diverse planten, mappen, persoonlijke koffiezetapparaten voor de medewerkers die geen genoegen konden nemen met de standaard koffieautomaten, foto's en allerlei andere prularia die de werkruimten een persoonlijke tint moesten geven.[235] Opvallend was ook dat er overal computers stonden van verschillend formaat en types, sommige exemplaren waren zeer verouderd. Op diverse computers zaten kleine gele plakpapiertjes. Toen ik aan mijn begeleidster vroeg waarom er zoveel verschillende computers stonden, antwoordde ze "*sommige computers worden gebruikt omdat dat daar oudere systemen op draaien die we niet goed kunnen overzetten naar de nieuwe computers. Om toch bij de gegevens te kunnen, houden we die oudere.*" Op de plakpapiertjes bleken in sommige gevallen later wachtwoorden te staan: ieder systeem had een eigen wachtwoord, en het was voor de gebruiker ondoenlijk om alle wachtwoorden te onthouden. De negatieve gevolgen voor de veiligheid van de systemen moest het in deze gevallen kennelijk afleggen tegen het gebruikersgemak. Inmiddels wordt er overigens gebruik gemaakt van één informatiesysteem, waarmee de noodzaak voor meerdere wachtwoorden is vervallen. De briefjes, met wachtwoorden althans, zullen vandaag de dag waarschijnlijk niet meer worden aangetroffen.

Na vier andere afdelingen, twee *koffie-corners* en vele meters aan archiefkasten te zijn gepasseerd, bereikten we de afdeling waar ik de komende drie jaar onderzoek zou gaan doen. De afdeling bevond zich aan het einde van de lange gang, en bestond uit een aantal kamertjes en een wat grotere, open ruimte. In totaal konden daar ongeveer tien man werken, wat me weinig leek voor een afdeling die formeel dertig mensen op de formatie had staan. Die plekken waren echter niet allemaal ingevuld, en in totaal werkten er ongeveer dertien mensen op de afdeling. Het team waar ik onderzoek zou gaan doen moest het centrale punt worden waar de CIE-informatie en de informatie uit andere bronnen (tactisch opsporingsonderzoeken, open bronnen en dergelijke) samenkomen. Dat team zou gaan bestaan uit analisten, wetenschappelijke onderzoekers en rechercheurs die vanuit verschillende disciplines de informatie zouden analyseren en vervolgens advies aan de stuurploeg zouden geven over de te volgen strategie ("*bookwise* en *streetwise* bij elkaar", aldus een leidinggevende). Ze stonden nog aan het begin van deze ontwikkeling, wat voor mijn onderzoek een mooi uitgangspunt was omdat ik dan bij de daadwerkelijke implementatie van IGP aanwezig kon zijn en het hele proces kon observeren. Verder was dat team belast met het monitoren van de voortgang in de lopende onderzoeken en moest het controleren of de van tevoren vastgestelde doelstellingen zouden worden behaald.

Mijn bureau stond tegenover dat van mijn begeleider op zijn kamer. Het was een vrij kleine kamer met overal dozen, kasten en dossiermappen. Op mijn bureau stonden nog foto's van degene die voor mij dat bureau had gebruikt. Aan de muur hingen een klein Surinaams vlaggetje en houtsnijwerk. Op het bureau stonden een paar boeken over de Antillen, Suriname, georganiseerde criminaliteit en een boekje van Geert Wilders. Mij werd verteld dat de rechercheur die aan dat bureau heeft gezeten net een tijdje in het buitenland was geweest, maar snel weer aan de slag zou gaan. Tot die tijd mocht ik zijn bureau gebruiken. Later in die week zou ik de betreffende rechercheur ontmoeten: een grote, zongebruinde man van middelbare

[235] Interessant zijn ook de politie-parafernalia die bepaalde medewerkers ten toon stellen: schildjes met het embleem van bevriende politiediensten, vlaggetjes, petten en dergelijke. Eén medewerker had zelfs een stuk schroot op een houten plankje met daarop het opschrift '*Katoesja Rocket*, Israël 2007'.

leeftijd, volgehangen met gouden sieraden en wanneer het kon met een zelfgedraaide sigaret in de mondhoek. Zijn accent lag ergens tussen Surinaams en plat Amsterdams. Dit zou later een soort mentor worden die ook de tijd nam om mij de Amsterdamse onderwereld te laten zien. Aan de muur tegenover mij hing een groot *whiteboard* waarop een gigantische onbegrijpelijke tekening van het werkproces van de organisatie stond. Dergelijke schema's en tekeningen zouden tijdens het onderzoek overigens veelvuldig terugkomen.

Mijn eerste indruk van de organisatie is misschien wel het beste te beschrijven als een zekere teleurstelling: het was allemaal heel normaal. In niets leek de organisatie op de rechercheafdelingen uit de televisieseries. Door de geïmproviseerde afscheidingen en pogingen om nog iets leuks van de werkplek te maken, kwam het een beetje chaotisch over.[236] Het beeld werd alleen nog maar bevestigd toen we bij de afdeling aankwamen waar ik onderzoek zou gaan doen. Het leek in alle opzichten op een doorsnee bedrijf met veel vergaderingen, overleggen, typische kantoorperikelen (zoals wie meer op het dak te vinden was dan achter het bureau: op het dakterras kon worden gerookt)[237] en geklaag over 'het management'. Maar wat tijdens de eerste weken echt opvallend was, was de openheid waarmee de medewerkers spraken over de organisatie, het werk, de leiding *et cetera*. Dit is het onderwerp van de volgende subsectie.

6.5.2 Acceptatie

Mijn grootste angst voordat ik aan de onderzoeksstage begon, was dat ik met name gezien zou worden als een hulpje, iemand die koffie mocht halen en mocht notuleren bij bepaalde vergaderingen. Niets bleek echter minder waar. Iedereen deed zijn best om mij zoveel mogelijk van informatie te voorzien en bijna iedere dag trof ik in mijn *email inbox* of op mijn bureau een document aan waarvan iemand dacht dat ik er wel wat aan zou hebben. De secretaresse regelde in twee dagen een toegangspas, een *email account*, autorisaties voor relevante computerbestanden *et cetera*. Misschien dat ze in die periode om wat voor een reden dan ook extra hun best deden om een goede indruk op mij achter te laten: volgens diverse medewerkers was alles voor mij uitzonderlijk snel geregeld. Zij vertelden vaak meer dan twee weken te moeten wachten op autorisaties en dergelijke. Maar ik kreeg niet het idee dat ze mooi weer speelden en mij iets voorspiegelden wat er niet was. Ik ben in de eerste week echter wel door een leidinggevende 'getest'. Dat ging als volgt.

Test en acceptatie

De eerste werkweek zat erop en, nog steeds onder de indruk van alle ervaringen, zat ik op een verjaardagsfeest van een familielid toen ik een sms-bericht kreeg van de hierboven genoemde leidinggevende. De tekst luidde: "*Ik bidde Allah voor vele geld, ikke krijge vele geld. Ik bidde Allah voor een dure auto, ikke krijge dure auto. Ik bidde Allah voor een grote lul, ikke krijge dit nummer.*"[238] Ik was een beetje van mijn à

[236] Een paar maanden later zou de organisatie verhuizen naar een nieuw pand. Dat zag er een stuk moderner en ruimtelijker uit, en is in alle opzichten een prettigere werkplek.

[237] Ik was zelf ook bijzonder veel op het dak te vinden: daar vonden de meest interessante gesprekken plaats. Vaak werd ik tijdens de rookpauzes geattendeerd op relevante ontwikkelingen voor mijn onderzoek en deed ik nieuwe contacten op. Het meeroken (ik rook zelf niet) en de kou nam ik op de koop toe.

[238] Mijn excuses voor het taalgebruik: binnen de politie worden dergelijke termen echter vaak gebruikt.

propos en wist niet zo goed wat ik ermee aan moest. Leidinggevenden op de universiteit hebben mij in ieder geval nooit zo bejegend, maar de politieorganisatie kent klaarblijkelijk hele andere omgangsnormen. Dezelfde leidinggevende had me bijvoorbeeld diezelfde dag een grafisch gedetailleerd verhaal verteld over een slachtoffer van een marteling/liquidatie die met een stuk gereedschap was bewerkt, en aan het einde van het verhaal zei hij "*ja jongen, tegen deze dingen moet je wel kunnen als je hier wil komen werken. Maar jij bent dit natuurlijk niet gewend, zo vers van de universiteit.*" Ik besloot dat de sms een test was, een manier om te peilen in hoeverre ik in de organisatie zou passen. Het leek me het verstandigst om maar direct te reageren met een slechte grap van mijn kant, en er volgde een korte sms-correspondentie. De maandag daarop werd ik door de leidinggevende begroet alsof hij me al jaren kende en we hebben onder het genot van een paar koppen koffie uitgebreid het weekend besproken. Hij vertelde me direct dat de organisatie wel 'slimmetjes' zoals ik zou kunnen gebruiken en beschreef alle mogelijkheden die de politie aan iemand met mijn profiel kon bieden. "*Maar wel eerst afstuderen jongen, das ook belangrijk.*"[239] Al snel na deze gebeurtenis werd mij medegedeeld dat ik betrokken zou worden bij een aantal lopende dossiers die mij inzicht zouden geven in de traditionele werkwijze van de recherche alsmede de nieuwe methoden die ze daar 'IGP' noemden. Er werd mij ook verteld dat 'eenmaal binnen bij de politie dan ben je ook echt binnen', wat volgens hem inhield dat 'er weinig geheimen zullen zijn' (behalve datgene dat juridisch en met name operationeel niet gedeeld kon worden). Dat hij dit serieus meende, bleek een week later. Ik werd toen door hem meegenomen naar een grote vergadering tussen een groep officieren van justitie en vertegenwoordigers van verschillende rechercheonderdelen van een aantal politiekorpsen. Het onderwerp was de regio-overschrijdende aanpak van de georganiseerde criminaliteit, en de bijeenkomst was erg operationeel van aard. Men begon met een voorstelrondje, en na een lange lijst van chefs zwacri, hoofden CIE, rechercheurs en officieren van justitie, kwamen ze bij mij aan. Ik stelde me eerlijk voor als een stagiaire die onderzoek deed naar IGP. Dit leidde tot opgetrokken wenkbrauwen en onderling gefluister tussen de aanwezigen. Ik zag twee officieren van justitie met elkaar overleggen en hun hoofd schudden terwijl ze naar mij keken. Het hoofd CIE dat naast mij zat fluisterde mij lachend in dat mijn aanwezigheid kennelijk niet goed viel. Ik werd echter niet weggestuurd en ben bij de hele vergadering aanwezig geweest. Dit is kenmerkend voor het vertrouwen dat ik vanaf het begin heb gekregen: ik werd meer gezien als een collega dan als een wetenschappelijke onderzoeker. Het is goed voor het vertrouwen en het verkrijgen van informatie voor het onderzoek, maar er is ook een risico aan verbonden. Het publiceren van de onderzoeksresultaten kan namelijk worden gezien als een soort van verraad of het schenden van een geheimhoudingsplicht. Ik heb daarom herhaaldelijk gewezen op mijn status als onderzoeker en dat wetenschappelijk onderzoek uiteindelijk openbaar is. Desondanks werd ik steeds meer gezien als collega en ook als zodanig behandeld.

[239] Gedurende de jaren waarin ik promotieonderzoek heb gedaan, is het me zelden gelukt om het verschil tussen afstuderen en promoveren uit te leggen. Uiteindelijk heb ik dit opgegeven, en ik moet zeggen dat de rol van student mij af en toe goed van pas is gekomen. Zo merkte ik bij een aantal collega's dat ze enigszins geïntimideerd leken te zijn door academische titels. Een student intimideert minder snel dan een 'wetenschapper'. Andere collega's wilden met name weten of het studentenleven echt zo heftig is als soms wordt voorgesteld en vonden een student binnen de gelederen eigenlijk wel interessant.

Op een gegeven moment kreeg ik overigens wel het idee dat ik soms door de leiding werd gebruikt als een soort academische *window-dressing*: ik werd soms naar bijeenkomsten gestuurd om het academische gehalte van de organisatie wat op te krikken. Dit zorgde ervoor dat ik in eerste instantie snel door de leiding werd geaccepteerd. Zo werd ik in de eerste maand meegenomen naar het managementteam-overleg waar de hoogste leiding het beleid van de organisatie besprak. Ik werd met open armen ontvangen en kreeg alle medewerking toegezegd. Later in de vergadering vroegen ze herhaaldelijk om mijn mening. Na de vergadering kwamen diverse leidinggevenden naar mij toe en vertelden dat ze het erg leuk vonden dat iemand met mijn profiel met ze wilde meedenken. Ik verbaasde me in die periode over de openheid waarmee men met mij sprak en de moeite die werd gedaan om mij duidelijk te maken dat ik mij op mijn gemak kon voelen. Het stond in schril contrast tot de waarschuwingen die mijn collega's van de universiteit mij in het begin hadden gegeven. Volgens hen zou ik worden gezien als een pottenkijker en vanwege mijn achtergrond niet worden geaccepteerd. Toen ik echter bij de CIE stage ging lopen, ging het opeens een stuk stroever.

De CIE

In het eerste jaar van mijn promotieonderzoek had ik aan een toenmalige collega verteld dat ik het liefste bij de CIE onderzoek deed. Hij vertelde mij dat dit onmogelijk is: daar kwam je volgens hem nooit binnen. Hij had het ook geprobeerd, en kreeg nul op het rekest. Ik had tijdens de stage echter goed contact met het hoofd CIE en een aantal medewerkers van de CIE, en besloot het er maar op te wagen en te vragen of het mogelijk was om daar stage te lopen. Tot mijn grote verbazing was het in één week geregeld. Technisch gezien was het een kleine aanpassing: er hoefde slechts een extra autorisatie op mijn toegangspas worden aangebracht. De echte uitdaging lag in de acceptatie bij de CIE. Dat was niet vanzelfsprekend. Ik werd in het begin niet geïntroduceerd bij de overige CIE-ers, hetgeen ertoe leidde dat sommige CIE-ers erg verbaasd waren om een nieuw gezicht te zien. Daarnaast zat ik op een klein kamertje, afgezonderd van de rest van de afdeling. Dit had een goede reden: ik kon niet op de kamer bij de runners zitten omdat die onderling met elkaar inhoudelijk over het werk spraken, en ik mocht daar niet bij zijn. Het zou me immers inzicht kunnen geven in de mogelijke identiteit van bepaalde informanten. De ontvangst was dan ook heel anders dan bij de informatieafdeling waar ik daarvoor onderzoek had gedaan.

Veel medewerkers van de CIE waren erg sceptisch over de door hen waargenomen trend binnen de politie om in toenemende mate jonge hoger opgeleide zij-instromers aan te nemen, en vonden duidelijk dat deze zich eerst in de praktijk moesten bewijzen. Dat gold ook voor mij, ondanks het feit dat ik daar als onderzoeker rondliep en niet als directe collega. Sterker nog, voor een aantal 'collega's' was ik daarom nog minder te vertrouwen: *"wat hebben we aan onderzoekers hier? Waarom worden er geen rechercheurs aangenomen?*" waren reacties die ik herhaaldelijk moest aanhoren. Tijdens één van mijn eerste inhoudelijke interviews kwam ik op de kamer van de respondent, een hoofd CIE. Hij was net in gesprek met zijn plaatsvervanger, een oude, ervaren politieman die zijn minachting voor academisch onderzoek niet onder stoelen of banken schoof. Mij werd toegeblaft "*wat kom je doen?*". Hij keek me verder niet aan en leek druk bezig met sms-en. Ik legde rustig uit dat ik zijn chef kwam interviewen, hetgeen klaarblijkelijk een fout was. "*Ik heb geen chef, ben m'n eigen baas*" was de reactie. Vervolgens stond hij op, nog steeds met

zijn telefoon in zijn hand en zijn blik daarop gericht, en mompelde "*ik heb geen tijd voor deze onzin. Ik ga werken, zou jij ook eens moeten proberen, 'chef*'." Mijn respondent keek me lachend aan terwijl zijn plaatsvervanger de kamer verliet. "*Wen hier maar aan, dit ga je nog wel een paar keer meemaken ben ik bang.*" Het interview was overigens bijzonder geslaagd.[240]

Ze waren er bij de CIE duidelijk niet aan gewend dat er mensen op de afdeling onderzoek deden naar werkwijzen en werkprocessen: deze worden doorgaans afgeschermd voor buitenstaanders. En dat ik een buitenstaander was, werd herhaaldelijk bevestigd. Zo was het op de informatieafdeling gebruikelijk dat er gezamenlijk werd geluncht. Dat gold ook voor de CIE. Het was dan ook een vreemde gewaarwording om rond lunchtijd de deur dicht te horen slaan en de enige te zijn die op de afdeling was achtergebleven. Toen vervolgens iemand met een dienblad vol koffie de kamers naast me binnen ging, maar die van mij oversloeg, werd me steeds duidelijker dat mijn aanwezigheid niet door alle CIE-ers werd geaccepteerd. Er zijn ook CIE-ers die gedurende die periode geen woord tegen me hebben gezegd. Het heeft me een aantal maanden gekost voordat ik eindelijk werd geaccepteerd door enkele medewerkers. Ik heb daarna aan een aantal CIE-ers gevraagd waarom ze zoveel moeite met mij hadden. Daarop kreeg ik veel verschillende antwoorden, waarbij er echter sprake was van één constante. Zoals één medewerker het verwoordde: "*je komt van de andere kant van de deur.*" Wat bleek het geval? Tussen de CIE en de RIO was een grote animositeit. Nu had ik wel wat kritische geluiden over de CIE gehoord, maar ik had mij nooit gerealiseerd hoe diep de problemen zaten. Van de RIO kwam de klacht dat de CIE zelden informatie deelt en onnodig geheimzinnig deed. De CIE-ers beweerden op hun beurt dat de RIO altijd de meest gevoelige 'dubbel nul' informatie verstrekt wilde hebben, maar dat dit juridisch niet kon en operationeel onverantwoord was. Omdat ik eerst bij de RIO onderzoek had gedaan, dachten sommige CIE-ers dat ik bij hun kwam om voor anderen te 'spioneren'. Toen eenmaal duidelijk was dat dit niet het geval was, verliep het contact aanmerkelijk soepeler. Uiteindelijk heb ik meer dan een half jaar onderzoek kunnen doen bij de CIE, en dat verliep op het einde net zo gemakkelijk als het onderzoek bij de RIO 'aan de andere kant van de deur'.

6.5.3 Een dynamische omgeving?

Dat de politieorganisatie wel degelijk een dynamische omgeving is, bleek toen er vanuit een criminele organisatie een mogelijke bedreiging jegens mijn stagebegeleider was. Hij kreeg tijdens een vergadering medegedeeld dat hij zijn vuurwapen bij zich moest dragen en extra moest opletten of hij iets verdachts zag. Bij het verlaten van de vergadering zei mijn stagebegeleider "*Thijs en ik gaan zo met de auto naar Den Bosch, we zijn vanmiddag tegen vieren weer terug. Kom je Thijs*?" Ik vroeg hem half serieus of hij het goed vond als ik hem op een veilige afstand zou volgen. Hij moest lachen en gaf aan dat ik hier niet van moest schrikken: dat hoorde volgens hem nu eenmaal bij het werk. Ik zal niet ontkennen dat ik het eigenlijk allemaal best spannend vond.

Het soort ervaringen zoals hierboven beschreven, weken bijzonder veel af van hetgeen ik gewend was op de universiteit. Al met al waren die eerste weken vol met nieuwe indrukken en soms spannende gebeurtenissen. Ik waande me af en toe op een

[240] Later bleek dit de specifieke humor van de CIE-er te zijn. Later doopte dezelfde man mij en een vrouwelijke collega al snel om tot Ken en Barbie.

filmset, waarbij de realiteit soms nog iets harder en vreemder leek dan de doorsnee politiefilm. Er werd continu een houding aangenomen alsof er ieder moment iets belangrijks stond te gebeuren, een soort permanente staat van paraatheid. Dat past ook wel bij de gemiddelde politiemedewerker die gewend is om op straat doorlopend te reageren op de omgeving en gezag uit te stralen. Het leidt tot een soort mentaliteit waarbij continu wordt gereageerd op de waan van de dag (zie ook subsectie 7.2.1). Later bleek dit overigens meer een aangeleerde houding te zijn, dan dat het daadwerkelijk een operationele noodzaak betrof.

Wat me namelijk na die enerverende eerste weken op begon te vallen, is hoe relatief normaal het werk bij een intelligence-organisatie eigenlijk is. De meeste dagen verlopen zonder noemenswaardige gebeurtenissen, en het werk laat zich nog het meest vergelijken met een typische kantoorbaan. Tijdens die normale weken heerst er echt een van negen tot vijf mentaliteit: wie na vijven door het pand loopt, treft doorgaans lege kamers aan. Er wordt bijzonder veel vergaderd en overlegd, hetgeen gepaard gaat met de inname van een ongezonde hoeveelheid koffie. Wat mij overigens is opgevallen als een groot verschil tussen de politie en de universiteit, is dat bij de politie vergaderen een onderdeel van het werk vormt terwijl het op de universiteit door de meeste medewerkers wordt gezien als een hinderlijke onderbreking van de werkdag. Vaak worden vakgroepvergaderingen afgesloten met de zin 'zo, en dan gaan we nu weer aan het werk'. Voor beide benaderingen is volgens mij wel wat te zeggen. We keren terug naar de stage.

Er ging bijna een jaar voorbij voordat er weer iets 'spannends' gebeurde. Voor een donderdag en een vrijdag ergens in 2008 stond een oefening gepland. Er zou een op handen zijnde terroristische aanslag worden gesimuleerd, en het team waar ik onderzoek bij deed zou de informatievoorziening voor zijn rekening nemen. Er was nog nooit een dergelijke oefening gedaan, dus het was voor de hele organisatie nieuw en spannend om te zien hoe zoiets zou lopen. Voor mij was het een mooie kans om te observeren hoe het informatieproces tijdens een (gesimuleerde) actie verliep, hetgeen voor mijn onderzoek wellicht nieuwe inzichten zou opleveren. Mij werd tijdens de oefening gevraagd of ik ze na de oefening wilde helpen met een evaluatie, ik was immers toch al bezig met het observeren voor mijn eigen onderzoek. Gedurende de oefening werd mij een aantal keren gevraagd of ik inhoudelijk kon helpen met bijvoorbeeld het zoeken van informatie op het internet. Op vrijdagmiddag was de oefening succesvol afgerond, en de week daarna zou ik gebruiken voor de evaluatie en om mensen te interviewen. De volgende dag werd ik echter in de middag gebeld door mijn stagebegeleider met het verzoek of ik direct in dienst wilde komen: "*stom toevallig, er loopt nu een echte terreurzaak, men raakt in paniek, iedereen moet komen helpen en we hebben jou ook nodig. Als je niet kunt komen, begrijp ik dat, maar we kunnen echt alle hulp gebruiken.*" Ik hoefde hier niet lang over na te denken: welke onderzoeker krijgt nu de kans om vanaf het begin een dergelijk politieel onderzoek mee te maken? Ik was enorm nieuwsgierig en vond het eigenlijk ook wel spannend. Achteraf bezien is dit het eerste echte moment van *going native* geweest. Ik was daar immers niet zozeer als onderzoeker, maar werd nu helemaal gezien als een onderdeel van het team. Eenmaal op de afdeling aangekomen was ik verbaasd over de wijze waarop ik werd benaderd door de leiding en de medewerkers. Ik was op dat moment voor hen geen onderzoeker meer, maar een collega.

Gedurende een aantal weken heeft iedereen op de afdeling lange werkdagen en –weken gedraaid, en ik deed daar aan mee. Wat me op dat moment opviel, was dat ik politiemensen zag werken in een *setting* waarin ze zich, vanuit het werk geredeneerd, op hun gemak voelden. Er was een calamiteit en er moest direct

gehandeld worden. De door mij tijdens het onderzoek gesignaleerde barrières die de vorming van een intelligenceorganisatie bij de politie tegenhouden, leken grotendeels te zijn weggevallen. Er werd eensgezind gewerkt aan de concrete zaak, de doelstellingen waren relatief duidelijk en men behoefde zich niet bezig te houden met een redelijk abstract concept (wat IGP voor veel politiemedewerkers nog steeds is, zie hoofdstuk zeven). Ik was de universiteit gewend en de relatieve (intellectuele) eenzaamheid van een promotieonderzoek. Voor mij was deze eerste ervaring met een concreet onderzoek dan ook echt overweldigend. De spanning, de tijdsdruk, de belangen en de snelheid van werken gecombineerd met een gevoel samen met anderen bezig te zijn aan zeer relevant werk waarbij ook direct resultaten zichtbaar waren: allemaal factoren die mij in één klap als het ware de politieorganisatie binnenzogen. Het duurde overigens nog een jaar voordat ik daadwerkelijk zou overstappen van de universiteit naar de politie. Dit brengt me tot een essentieel onderwerp van dit hoofdstuk: het risico dat antropologen het gevaar van '*going native*' noemen.

6.5.4 Tot slot: *Going native?*

Ik sluit dit hoofdstuk af met een behandeling van het grote risico van ons type onderzoek: het *going native*. Ik ben in maart 2009 overgestapt van de universiteit naar de politie. Hiervoor zijn meerdere redenen te geven, maar ik beperk me tot de belangrijkste. Zoals ik reeds heb beschreven, voelde ik mij bijzonder aangetrokken tot bepaalde aspecten van het politiewerk, zoals de saamhorigheid tijdens calamiteiten, het feit dat je snel resultaat van je werk ziet en zeker ook de (schaarse momenten van) spanning. Kort gezegd wilde ik niet langer aan de zijlijn staan als onderzoeker, maar ik wilde een onderdeel van de organisatie worden. Hier schuilt het bovengenoemde gevaar van *going native*: door over te stappen naar de politieorganisatie waar ik onderzoek naar heb verricht, kunnen vraagtekens worden gezet bij mijn objectiviteit en onafhankelijkheid. Dit hoeft overigens niet alleen te betekenen dat ik minder kritisch ben naar de organisatie. Het tegendeel is immers ook mogelijk: dat ik (onterecht) te kritisch ben vanwege bepaalde frustraties die je als medewerker nu eenmaal zult ervaren. Los van de vraag of ik al dan niet te kritisch ben: het feit dat ik bij de politieorganisatie ben gaan werken, kan wellicht worden gezien als een overmatige identificatie met de onderzoeksgroep en dus mogelijk tot *going native*. Maar wat houdt *going native* eigenlijk in?

Going native houdt in dat de onderzoeker zich teveel identificeert met zijn onderzoekssubjecten en op een bepaald moment onderdeel daarvan wordt in plaats van dat hij een objectieve en afstandelijke (wetenschappelijke) houding aanneemt. Met andere woorden: er is sprake van een overmatige identificatie met de onderzoeksgroep. Dit is met name een risico wanneer bij participerende observatie, hetgeen de kern vormt van het antropologisch onderzoek, de nadruk steeds meer gaat liggen op participatie en de observatie minder belangrijk wordt. Enige identificatie met de onderzoeksgroep is echter wel degelijk nodig. In de sociologie noemt men dit '*Verstehen*'. Het is een proces van subjectieve interpretatie door de onderzoeker, "*a degree of sympathetic understanding between social researcher and subjects of study, whereby the researcher comes to share, in part, the situated meanings and experiences of those under scrutiny*" (Ferrell 1998: 27). Dat dit een zekere mate van subjectiviteit met zich meebrengt, is onvermijdelijk. Volgens sommigen wordt het van de etnograaf verwacht dat hij zich als het ware onderdompelt in het door hem bestudeerde fenomeen, waarbij de sleutel van succes ligt in het 'onderdompelen met

behoud van objectiviteit', oftewel een soort betrokken distantie (zie Jacobs 1998: 164).

Er is echter een belangrijk probleem met het *going native* idee. Het is namelijk erg moeilijk om vast te stellen wanneer er sprake is van een 'overmatige identificatie met de onderzoeksgroep'. Wanneer gaat een gewone identificatie over naar een overmatige variant? Dit hoeft niet het geval te zijn bij een overstap van de universiteit naar de politie zoals ik heb gedaan: het feit dat ik me deels identificeer met de politieorganisatie betekent nog niet dat ik me overmatig identificeer. In het verlengde hiervan ligt het tweede probleem: de subjectiviteit van de beoordeling of er sprake is van een overmatige identificatie. Dit zal immers per persoon verschillen, hetgeen te maken kan hebben met bijvoorbeeld de wetenschappelijke discipline waartoe iemand behoort. Zo zal een exacte wetenschapper de identificatie en de bijbehorende subjectiviteit wellicht sneller als overmatig en een aantasting van de wetenschappelijke waarde van een onderzoek beoordelen dan een sociale wetenschapper.

De vraag rijst nu hoe ver mijn identificatie met de onderzoeksgroep is gegaan. Wanneer een onderzoeker de grens overgaat, is van tevoren nauwelijks vast te stellen. Wij (mijn promotores en ik) hebben geprobeerd om zo goed en zo kwaad mogelijk bepaalde waarborgen in te bouwen. Ten eerste hadden wij periodieke bijeenkomsten waarbij ik en de promotores het project doorspraken. Hierbij kwamen de problemen waarmee een veldwerk-onderzoek in aanraking komt aan bod. Daaronder aspecten van '*going native*'. Ten tweede heb ik gedurende de hele onderzoeksperiode een dagboek bijgehouden waarin ik veel aandacht heb geschonken aan subjectieve aspecten van het onderzoek. Hiermee ben ik ook na de overstap van de universiteit naar de politie doorgegaan, omdat het van belang is om de relevante subjectieve aspecten van veldwerkonderzoek in het oog te houden. Ook tijdens de fase van de analyse van de data ben ik me dus bewust geweest van de mogelijke subjectieve factoren die de analyse zouden kunnen beïnvloeden. En voor zover *going native* verwijst naar de mate waarin de onderzoeker daadwerkelijk een *native* wordt, en zich dus gaat vereenzelvigen (of wordt vereenzelvigd) met de onderzoeksgroep is er in mijn gevoel een bijkomend voordeel. Iemand met mijn profiel (een academische achtergrond) wijkt in belangrijke mate af van de rest van de onderzoeksgroep (de traditionele politiemedewerker). Van een vereenzelviging is dan ook in dit opzicht geen sprake.

Er zitten zeker ook voordelen aan de overstap naar de politie. Het eerste voordeel is dat je als medewerker sneller wordt vertrouwd door andere politiemedewerkers, en dit maakte het aanzienlijk makkelijker om de juiste respondenten te selecteren en interviews af te nemen. Het zorgt er ook voor dat er minder sprake is van reactiviteit van de kant van de onderzoeksgroep: zij zullen het gedrag tijdens het werk minder snel aanpassen omdat ze worden geobserveerd door een onderzoeker. Dit verhoogt de validiteit van het onderzoek. Ik moet hierbij opmerken dat mijn observaties tijdens mijn dagelijkse werkzaamheden in dienst van de politieorganisatie slechts zijn gebruikt als sturingsinformatie voor de interviews en als falsificatie en verificatie van eerdere onderzoeksbevindingen.

Inmiddels ben ik sinds 1 januari 2010 werkzaam bij een ander politiekorps. In deze nieuwe rol heb ik geen observaties meer verricht. Mijn huidige werkgever is immers nooit partij geweest bij de aan het begin van het onderzoek gemaakte afspraken en behoort dan ook niet tot mijn onderzoeksgroep. Indien ik hier participerende observaties zou verrichten, zou dit neerkomen op 'spioneren' in plaats

van wetenschappelijk onderzoek. Daarnaast zou het problematisch zijn in het licht van mijn ambtelijke integriteit.

Al met al ben ik van mening dat mijn overstap van de universiteit naar de politie niet gezien moet worden als *going native* in de negatieve zin van het woord. Ik ben me tijdens het onderzoek bewust geweest van dit gevaar, en heb de participatie nooit boven de observaties geplaatst. Ik hoop dat dit voldoende volgt uit de volgende twee hoofdstukken.

7| IGP in de praktijk

In dit hoofdstuk behandelen wij IGP in de CIE-praktijk en beantwoorden wij OV3: *In hoeverre is IGP geïmplementeerd in de Nederlandse CIE-praktijk*? We analyseren in hoeverre de uitgangspunten van IGP in de praktijk van de bestrijding van georganiseerde criminaliteit en terrorisme daadwerkelijk zijn en/of worden geïmplementeerd. In sectie 5.4 hebben wij IGP beschreven als een model waarbij (1) criminaliteitsanalyse leidt tot de opbouw en instandhouding van een informatiepositie welke (3) de besluitvorming faciliteert en waarbij (4) informatie zoveel mogelijk wordt gedeeld, dit alles ten behoeve van (2) een proactieve werkwijze en preventieve aanpak van criminaliteit (en terrorisme).

In dit hoofdstuk bezien wij in hoeverre wij dit model in de praktijk hebben waargenomen. Hiertoe beschrijven we allereerst wat de politiemedewerkers in de praktijk verstaan onder IGP (sectie 7.1). De mate waarin de werkvloer op de hoogte is van het concept is van belang voor het beoordelen van de achtergronden en oorzaken van het al dan niet accepteren van IGP.

Eén van de belangrijkste aspecten van IGP is sturing. Het concept beoogt het politiewerk gericht te sturen. Sturing van de politieorganisatie is volgens wetenschappelijk onderzoek bijzonder lastig (zie Lipsky 1980; De Hert et al. 2005: 368; Van der Vijver en Terpstra 2007: 366-370), en de vraag is dan ook in hoeverre de politie in de praktijk daadwerkelijk gestuurd kan worden. De praktijk van de sturing is het onderwerp van sectie 7.2. Vervolgens behandelen we de drie verschillende fasen van het informatieproces, te weten verzamelen, verwerken, en verstrekken. IGP zorgt voor een verandering in al deze fasen. Met betrekking tot de verzameling van informatie beantwoorden wij de vraag in hoeverre de verzameling van informatie proactief is (sectie 7.3). Na de verzameling van informatie behandelen we de verwerking van informatie (sectie 7.4). In deze sectie staat de vraag centraal hoe de politie in de praktijk omgaat met de toenemende informatiestromen en welke rol criminaliteitsanalyse speelt in de praktijk van de CIE en het informatieproces. Vervolgens beschrijven wij de praktijk van het verstrekken van informatie: de ontwikkeling naar *need to share* (sectie 7.5). Wij beantwoorden de vraag "in hoeverre is *need to share* een onderdeel van de politiepraktijk?" Tot slot geven wij het antwoord op OV3 in sectie 7.6 tezamen met andere hoofdstukconclusies.

De voor dit hoofdstuk relevante theoretische concepten en inzichten hebben wij reeds in hoofdstukken twee en vijf behandeld. Wij zullen indien nodig naar deze hoofdstukken verwijzen.

Een laatste opmerking betreft de opzet van de secties: wij sluiten alle secties af met een concluderende subsectie, genaamd tussenconclusie. In deze subsecties verwoorden wij onze tussenconclusies in de vorm van praktijkbevindingen. Deze praktijkbevindingen werken wij uiteindelijk om tot een algemene conclusie en een antwoord op OV3.

7.1 Wat is IGP?

Wij hebben de respondenten onder meer gevraagd naar wat zij verstaan onder IGP.[241] In deze subsectie gaan wij hier kort op in, en geven wij aan waar de verschillen zitten

[241] Zie subsectie 6.2.3 voor een overzicht van de respondenten en een verdere methodologische verantwoording.

met de door ons gehanteerde definitie. Uit de antwoorden volgt dat er uiteenlopende zienswijzen bestaan omtrent IGP en wat eronder moet worden verstaan. Iedereen geeft er een eigen invulling aan. Wij constateren dat er (7.1.1) onduidelijkheid is bij de respondenten omtrent wat IGP is, (7.1.2) de meeste respondenten IGP zien als proces gericht op de productie van verschillende soorten informatie (de productbenadering) en (7.1.3) de voorwaarschuwingsfunctie van IGP niet duidelijk naar voren komt maar verborgen is.

7.1.1 Onduidelijkheid omtrent IGP

Het valt op dat er veel verschillen zijn tussen de opvattingen over wat IGP precies is. Eén van de respondenten formuleert het als volgt.

"*Definieer intelligence led policing maar eens. Waar hebben we het over? (…) Alles in het politiewerk draait om info, info, info."* Interview hoofd CIE (A), mei 2007.

Deze respondent geeft aan dat IGP in essentie draait om informatie, maar hij zegt tegelijkertijd dat *alles* binnen de politie om informatie draait. Een duidelijke definitie kon deze respondent verder niet geven, en dat geldt voor vrijwel alle respondenten. Maar het gaat bij IGP volgens hen in de kern dus om informatie. Overigens geven diverse respondenten aan dat dit niet nieuw is, maar vroeger ook al het geval was. Een analist verwoordt het als volgt.

"*Er is altijd wel een vorm van IGP geweest. Toen we kaartenbakjes hadden, waren er ook rechercheurs die probeerden om de info zo gestroomlijnd mogelijk te krijgen en in het rechercheproces te integreren. Dat is geen nieuwe gedachte.*" Interview CIE analist CIE (G), maart 2011.

Meerdere respondenten geven net als de hiervoor aangehaalde rechercheur aan dat IGP niet echt nieuw is voor de politie. Het is iets dat al langer wordt gedaan. Zij vatten IGP erg letterlijk op en ontlenen de definitie aan de hand van de precieze betekenis van de verschillende onderdelen van de term (informatie, sturing en politiewerk).

"*(IGP) is een modewoord omdat politiewerk altijd al informatiegestuurd is geweest. Je hebt informatie gewoon nodig voor het opstarten van een zaak en het doen van onderzoeken.*" Interview teamleider RIO (A), januari 2008.

Het is essentieel om bij de beginfase van veranderingen een duidelijke toekomstvisie voor ogen te hebben: "*zonder een globale veranderingsvisie dreigt een veranderingspoging immers te verworden tot een verzameling verwarrende en op zichzelf staande projecten die de organisatie niet ten goede komen*." (Maesschalck 2008: 1). Bij IGP lijkt er dus geen duidelijke visie te zijn, althans niet op de werkvloer. Het is voor de medewerkers lang niet altijd duidelijk wat er met IGP wordt bedoeld. We constateren dan ook dat vrijwel alle respondenten IGP zelfstandig invullen. Uit onze observaties blijkt voorts dat de term IGP (of IGO) wordt gebruikt voor veel verschillende onderwerpen. Veel 'innovaties', zoals nieuwe analysemethoden en nieuwe technologieën, worden onder de noemer van IGP geschaard omdat ze iets met het informatieproces te maken zouden hebben. In het ene geval is dit terecht, omdat de innovatie daadwerkelijk ziet op een aspect dat relevant

is voor IGP, zoals *datamining*. In andere gevallen wordt IGP als een soort label geplakt op ontwikkelingen die in de kern weinig tot niets met het oorspronkelijke concept van IGP te maken hebben. Het concept is daarmee onderhevig aan *netwidening*. Dit wordt duidelijk wanneer naar de historische ontwikkeling van het concept wordt gekeken. In eerste instantie werd gesproken van *intelligence-led policing*, wat al vrij snel werd omgedoopt tot de informatiegestuurde opsporing (zie De Hert en Vis 2005). Informatiegestuurde opsporing werd vervangen door informatiegestuurde politie, waardoor naast de opsporing ook de andere politietaken onder het bereik van het concept werden gebracht (zie De Hert et al. 2005). Maar hier bleef het niet bij. Al snel werd er gesproken van informatiegestuurde veiligheidszorg, waarbij niet alleen op het politiewerk maar ook op de veiligheidstaak van andere publieke organisaties (zoals de gemeenten) werd gedoeld (zie Versteegh 2005). Vandaag de dag wordt de term intelligencegestuurde politie (IGP) gehanteerd, de term die wij ook in dit boek gebruiken (zie ook Kop en Klerks 2009; Den Hengst-Bruggeling 2010). IGP wordt gedefinieerd via iedere keten van de politieorganisatie (en daarbuiten). Deze ketens hebben allemaal een eigen benadering en leggen de nadruk op andere elementen, waardoor de uiteindelijke uitwerking van IGP de kans loopt weinig meer van doen te hebben met het idee achter het oorspronkelijk concept. Dit moet goed bewaakt worden.

Er is dus geen eenduidige visie op IGP. Dit behoeft echter niet automatisch te leiden tot grote problemen voor de implementatie van IGP. In beleidsliteratuur worden verschillende voorwaarden genoemd waaraan moet zijn voldaan wil een ambigu containerbegrip zoals IGP succesvol worden geïmplementeerd (zie voor een overzicht van deze literatuur Maesschalck 2008). Zo moet er ten eerste (A) sprake zijn van concrete en goed uitgewerkte voorstellen die op een geloofwaardige manier aan het containerbegrip kunnen worden gekoppeld. Op zichzelf kan een zekere ambiguïteit overigens ook een voordeel zijn, met name wanneer het wordt gebruikt om veel verschillende partijen achter de (vermeende) noodzakelijke verandering te krijgen. Dat gaat nu eenmaal gemakkelijker wanneer de beoogde verandering niet te eenduidig is. Het wordt echter problematisch wanneer een abstract concept daadwerkelijk moet worden vertaald naar een concrete beleidsbeslissing (Maesschalck 2008: 5). We merken hierbij op dat er grote problemen zouden kunnen ontstaan als de beoogde visie inhoudelijk wordt aangepast aan de wensen van specifieke partijen. Hiervan lijkt bij IGP mogelijk sprake te zijn.

Ten tweede (B) biedt het abstracte concept van IGP een mogelijke oplossing voor min of meer abstracte problemen, zoals hoe als politie om te gaan met de eisen van een risicosamenleving. Dit voordeel behoeft nuancering. Abstracte problemen zijn namelijk geen problemen waarmee de werkvloer en middenkader van de leidinggevenden zich dagelijks bezighouden. Deze twee invalshoeken brengen ons tot het volgende. Iedere schakel in de keten waarlangs het concept gaat om geïmplementeerd te worden, heeft invloed op de uitwerking en implementatie van dat concept, hetgeen uiteindelijk leidt tot veel verschillen in definities en implementaties (Peters 2001: 231). Het gevolg van deze *netwidening* is dan ook dat het concept zo breed wordt toegepast, dat het (1) geen onderscheidend vermogen meer heeft, (2) dat het concept steeds minder gelijkenis vertoont met het oorspronkelijke idee waarop het is gebaseerd en (3) dat het steeds moeilijker wordt om te beoordelen wanneer er sprake is van een succesvolle implementatie (zie ook: De Hert et al. 2005).[242] Wij constateren dat beide gevolgen voor IGP gelden.

[242] Zie sectie 1.2 voor de definities die wij in ons onderzoek hanteren.

Wat precies onder IGP moet worden verstaan, is dus onduidelijk. Wat wel duidelijk is, is dat IGP het politiebestel grondig probeert te hervormen. Niet voor niets wordt er soms gesproken van 'een paradigmawijziging' (Ratcliffe 2008; zie ook subsectie 1.1.2). In deze ambitie met IGP schuilt volgens ons een gevaar.

Het theoretische sociaalpsychologische model van de sociale identiteit biedt inzicht in hoe individuen in een organisatie zichzelf een identiteit aanmeten (of aangemeten krijgen). Volgens deze theorie is een belangrijke functie van een organisatie het verlenen van een sociale identiteit aan leden van de organisatie. Deze personen ontlenen status en eigenwaarde aan de status van de organisatie waartoe zij behoren. De theorie van de sociale identiteit geeft echter niet zozeer inzicht in de wijze waarop groepsleden eigenschappen aan de eigen groep ten opzichte van andere groepen toeschrijven: dat doet de nog te behandelen theorie van sociale categorisatie (zie subsectie 7.5.3). De theorie van de sociale identiteit richt zich op hoe het lidmaatschap van een groep wordt gevormd door zaken als identiteit en status, en richt zich met name op processen die binnen een groep plaatsvinden (zie Tyler 2001: 154-155). Problemen met betrekking tot de implementatie van IGP kunnen wellicht worden verklaard met behulp van de theorie van de sociale identiteit. Zo stelt deze theorie (kort gezegd) dat gedrag dat voor een organisatie positief is, afhangt van de mate van identificatie van groepsleden met de organisatie. Dergelijk gedrag kan (1) dwingend worden opgelegd en afgedwongen door middel van beloningen en straffen of (2) voortkomen uit een eigen motivatie, en het gevolg zijn van bepaalde interne opvattingen en waarden (Tyler 2001: 152 e.v.). Met name daar waar de groepsleden een grote discretionaire ruimte hebben, zoals bij de politie en andere *street-level* bureaucratieën, is positief gedrag afhankelijk van de eigen motivatie van de groepsleden. Acceptatie van IGP of elementen daarvan zijn, wanneer we het perspectief van de politieorganisatie in het algemeen kiezen, met name afhankelijk van de eigen motivatie van de medewerker. En dit kan problematisch worden wanneer IGP uiteindelijk in de ogen van (een categorie van) medewerkers de kenmerken van de organisatie waaraan zij hun identiteit ontlenen zal veranderen. Een fundamentele verandering in de identiteit van de organisatie heeft fundamentele gevolgen voor sociale identiteit van de medewerkers. Als de politieorganisatie niet langer datgene vertegenwoordigt waar (een categorie van) medewerkers hun identiteit aan ontlenen, dan zal het waarschijnlijke gevolg zijn dat deze medewerkers niet snel 'positief gedrag' vertonen. In deze situatie zal de politieleiding zich in toenemende mate moeten verlaten op dwang door middel van beloningen en straffen. Dat dit vrijwel onmogelijk is vanwege de omgekeerde feitelijke hiërarchie binnen de politieorganisatie, zullen wij nog in subsectie 7.2.2 behandelen. Hier volstaan we met de waarschuwing aan de voorvechters van IGP dat tè verregaande veranderingen zullen leiden tot verminderde identificatie, meer verzet en uiteindelijk minder effectief en efficiënt politiewerk. Wij merken echter op dat wij op basis van ons onderzoek niet kunnen vaststellen of, en zo ja, in hoeverre hiervan in de Nederlandse situatie sprake is. Hiervoor is immers meer en specifieker onderzoek nodig naar de werking van de sociale identiteit binnen de politie, en zullen andere onderzoeksmethoden dan die van ons, zoals enquêtes of specifiek op de sociale identiteit toegesneden interviews, wellicht tot betere resultaten leiden. Het lijkt ons evenwel evident dat een verandering van 'doen' naar 'denken' zoals met IGP wordt beoogd een verregaande verandering is met in potentie verregaande gevolgen voor de sociale identiteit van de politiemedewerker.

7.1.2 IGP als informatieproduct (de product-benadering)

In subsectie 5.4.7 hebben wij de politiële visie op intelligence behandeld, en hebben wij vastgesteld dat de politie een piramidale structuur hanteert waarbij intelligence een modaliteit van informatie is. In deze benadering ligt de nadruk met name op het productieproces van intelligence, en wordt er minder uitgegaan van de uiteindelijke doelstelling van intelligence. In vrijwel alle interviews komt een variant van deze productbenadering terug. Meerdere respondenten wijzen bijvoorbeeld op het verschil tussen de zachte informatie die de CIE verzamelt, en de harde informatie die de tactische opsporingsteams verzamelen. Het onderscheid tussen zachte en harde informatie speelt volgens deze respondenten een belangrijke rol bij IGP. De volgende respondent meent dat IGP met name geënt zou moeten zijn op harde informatie.

"*Er bestaat ook een verschil in informatie, data en intelligence, en de letterlijke vertaling van intelligence is natuurlijk inlichtingen, hetgeen weer een andere betekenis heeft. Je zit dan in de sfeer van het inlichtingenwerk en de zachte informatie. Hier ligt een kernpunt: als je alles om informatie laat draaien, dan moet je een onderscheid maken tussen harde en zachte informatie (…) Tegenwoordig wordt echter het 'intelligence' element van ILP losgelaten en wordt er meer geïnvesteerd in de knowledge kant ervan: knowledge led policing, zeg maar.*" Interview hoofd CIE (A), mei 2007.

Een andere respondent formuleert het als volgt.

"*(…) intelligence associeer ik met het CIE-matige, de inlichtingenkant van het werk. Terwijl ik informatie zie als het geheel van inlichtingen en tactische informatie. En volgens mij is dat wat je het liefste wil, want je moet je niet laten sturen door alleen maar inlichtingen van bronnen. Je moet vanuit het hele plaatje je opsporing gaan sturen.* (De term) *informatiegestuurd is denk ik zuiverder dan intelligencegestuurd.*" Interview recherchekundige RIO (A), mei 2010.

Dit is een belangrijke aanwijzing voor de rol van de CIE in het concept IGP. Essentiële kenmerken van het CIE-werk, zoals geheimhouding, staan op gespannen voet met bepaalde uitgangspunten van IGP zoals *need to share* (zie ook sectie 7.6).

Er zijn ook respondenten die de nadruk leggen op andere vormen van informatie, zoals informatie uit open bronnen.

"*Intelligence-led policing klinkt wel mooi en interessant, maar wat is het? Er zijn verschillende soorten informatie waar de politie mee werkt. Hoe ziet een intelligence-led politie eruit?" (Wij zijn) met name bezig met het bij elkaar brengen van opsporingsinformatie. Open bronnen worden niet gebruikt.*" Interview teamleider tactiek (A), december 2007.

In andere interviews worden wij door analisten gewezen op het belang van de toegang tot alle informatie voor een zo volledig mogelijke analyse. Zij zien IGP als een nieuwe informatie-infrastructuur die meer informatie toegankelijk maakt voor de medewerkers. De aspecten die de respondenten benadrukken, hangen af van de functie van de desbetreffende respondent: CIE-ers zien een belangrijke rol voor de CIE-informatie, tactische medewerkers noemen het belang van tactische informatie *et cetera*.

Een rode draad door alle interviews heen is dat de respondenten in vrijwel alle gevallen een variant van de politiële definitie hanteren, te weten de visie op IGP als een concept dat draait om een modaliteit van informatie (zie subsectie 5.4.7). Wij constateren dat de meeste respondenten IGP vrij pragmatisch benaderen, hetgeen een verklaring kan zijn voor de focus op de productbenadering.

7.1.3 IGP als voorwaarschuwing (de intelligence-benadering)

In hoofdstuk vijf hebben wij onze definitie van intelligence gegeven, en beargumenteerd dat intelligence bedoeld is om voorwaarschuwingen te geven. Dit vormt de grote aantrekkingskracht van het concept op de politie (subsectie 5.4.7). Opvallend is echter dat slechts een enkele respondent tijdens de interviews uit zichzelf het geven van voorwaarschuwingen noemt als element van IGP.

"*intelligence is bedoeld om naar voren te kijken. Een voorbeeld is het NDB: we hebben gesproken met een groot aantal experts en hen gevraagd wat we kunnen verwachten op het gebied van georganiseerde criminaliteit. (…) Je moet ook achterom kunnen kijken om iets over de toekomst te kunnen zeggen. Naar voren kijken en zaken voorkomen is wel essentieel. Intelligence is ook actiegerichte informatie. Je moet er iets mee kunnen doen. Er is een grote stroom informatie die je actiegericht moet maken.*" Interview projectmedewerker IGP (A), februari 2008.

Het bovenstaande citaat is echter een uitzondering: verreweg het merendeel van de respondenten benoemde de voorwaarschuwingsfunctie niet wanneer ze werden gevraagd om het doel van IGP te omschrijven. In de dagelijkse politiepraktijk spreekt men echter wel vaak over een vorm van voorwaarschuwingen. Wij vernamen in de wandelgangen, bij de koffiebesprekingen en bij vergaderingen herhaaldelijk dat men de wens had om 'meer aan de voorkant van criminaliteit' te komen (dus proactief te werken) en minder afhankelijk te worden van de waan van de dag. Dit blijkt ook uit de diverse initiatieven die worden ondernomen om, bijvoorbeeld in het kader van *pilot*-onderzoeken, indicatoren op te stellen van bijvoorbeeld radicalisering en deze te integreren met geavanceerde *datamining* programma's en andere technologieën.[243] De medewerkers verbinden dit echter niet direct met het concept van IGP. De voorwaarschuwingsfunctie ligt als het ware verborgen in het concept. Een verklaring hiervoor ligt in het verlengde van de bovengenoemde verklaring voor de focus op de productbenadering: om een pragmatisch oordeel te kunnen geven over IGP, vallen de meeste politiemensen terug op de eigen werkervaring en het daarop gebaseerde referentiekader. Voorwaarschuwingen hebben echter nooit tot de dagelijkse werkzaamheden gehoord en zijn geen onderdeel van dat referentiekader. Zij worden dan ook niet verbonden met IGP. De meeste respondenten beoordelen IGP aan de hand van het bestaande werkproces en zien het met name als een oplossing voor tekortkomingen binnen dat bestaande (traditionele) werkproces. Een geheel nieuw element zoals voorwaarschuwingen valt dus buiten de belevingswereld van de gemiddelde politieman, zo blijkt uit onze observaties en interviews. Een uitzondering vormen overigens de respondenten die nauw betrokken zijn bij het ontwikkelen van IGP: zij leggen doorgaans wel de link met voorwaarschuwingen en zien hierin een belangrijke doelstelling voor IGP (zie de hierboven aangehaalde respondent). Wij

[243] Omdat de politie wordt geteisterd door ICT-problemen die de ambities van deze initiatieven tegenwerken, ontstijgen deze projecten zelden de status van *pilot*.

verwachten dat dit verandert op het moment dat er meer operationele ervaring komt met voorwaarschuwingen en de meerwaarde daarvan.

Men denkt dus met name in bepaalde soorten informatie (hard/zacht, politie/open) en wat ermee dient te gebeuren (delen) wanneer ze wordt gevraagd naar wat IGP inhoudt. Wat het uiteindelijke doel van IGP is, wordt nauwelijks benoemd.

7.1.4 Tussenconclusies

Naar aanleiding van ons veldwerk komen wij tot de volgende tussenconclusies die wij weergeven als praktijkbevindingen:

Praktijkbevinding 1a: Er is geen eenduidige opvatting op de werkvloer over wat IGP is. Afhankelijk van de functie van de betreffende medewerker of het organisatieonderdeel waar hij werkzaam is, krijgt het concept bepaalde kenmerken toebedeeld.

Praktijkbevinding 1b: IGP wordt met name ingevuld vanuit een productbenadering. De intelligencebenadering met de nadruk op het geven van voorwaarschuwingen wordt niet expliciet in verband gebracht met IGP, maar vindt verspreid over de organisatie toch plaats.

Praktijkbevinding 1c: IGP wordt als label gebruikt voor ontwikkelingen die in relatie staan tot het informatieproces van de politie, en is in dat opzicht onderhevig aan een verregaande *netwidening*.

Concluderend

We kunnen vaststellen dat alle respondenten van IGP hebben gehoord. Het concept is bekend bij de medewerkers. Er zijn echter bijna net zoveel benaderingen van IGP als er functies binnen de politie zijn. Omdat het voor de medewerkers op de werkvloer en de leidinggevenden niet duidelijk is wat er precies onder IGP moet worden verstaan, wordt de implementatie van het concept aanzienlijk bemoeilijkt. In naam wordt er al snel volgens IGP gewerkt, maar het is de vraag of dit in realiteit ook het geval is. Wij constateren dan ook een verschil tussen de beleving van de werkvloer omtrent IGP en de officiële benadering.

7.2 Sturing in de praktijk

IGP wordt door de politie met name gezien als een sturingsconcept (zie subsectie 5.4.3). Sturing binnen IGP valt uiteen in twee belangrijke delen. Het eerste deel is de sturing op strategisch niveau. Dit betreft het vaststellen van de algemene prioriteiten en het verdelen van de capaciteit. Dit kan worden gezien als het beantwoorden van de ‘wat-vraag’: wat gaat het korps of de CIE doen? Het tweede deel is de operationele en tactische sturing: de sturing van de dagelijkse werkzaamheden. Dit is het beantwoorden van de ‘hoe-vraag’: hoe gaat het korps of de CIE de prioriteiten daadwerkelijk uitvoeren? Wij behandelen in deze sectie allereerst de strategische sturing (subsectie 7.2.1). Daarna gaan wij in op de operationele/tactische sturing (subsectie 7.2.2). In deze sectie laten wij de vraag in hoeverre de sturing plaatsvindt op basis van analyseproducten buiten beschouwing. Dat komt aan bod in sectie 7.4 waarin we de analyse behandelen.

7.2.1 De strategische sturing

De Nederlandse uitwerking en invulling van IGP is het NIM. Het NIM geeft onder meer een invulling aan de beleidsomgeving van de politie. In subsectie 5.4.2 hebben we aangegeven hoe de beleidsomgeving van de Nederlandse politie er volgens het NIM uit zou moeten zien. Er dient een stelsel van stuurploegen en weegploegen te komen die op een strategisch niveau de politieorganisatie aansturen. De vraag is nu in hoeverre dat stelsel van stuur- en weegploegen in de praktijk functioneert en hoe de CIE en de RIO in het algemeen op strategisch niveau worden aangestuurd. Wij behandelen in deze subsectie achtereenvolgens (A) de strategische stuurploegen, (B) de verschillen tussen de korpsen in het zwacribeleid, (C) de rol van de CIE bij beleidsvorming, (D) de prestatiesturing en (E) de waan van de dag.

A: De strategische stuurploegen

De strategische stuurploegen zijn inmiddels (2012) bij diverse korpsen in het leven geroepen en zij functioneren op strategisch niveau al vrij goed. Zo worden er landelijk prioriteiten vastgesteld door een landelijke stuurploeg en stellen de regionale stuurploegen de prioriteiten voor de regio's vast. Wij hebben geen zicht gehad op het functioneren van de landelijke stuurploeg anders dan dat wij hebben geconstateerd dat er landelijk bepaalde prioriteiten zijn geformuleerd waar de aandacht van de politie naar uit dient te gaan.[244]

Bij de organisaties waar wij ons onderzoek hebben uitgevoerd, nemen de stuurploegen een belangrijke positie in het besluitvormingsproces in. Zij stellen een soort raamwerk voor de prioriteiten vast waarop de verschillende onderdelen zich dienen te gaan richten. In de stuurploeg wordt onder meer besloten welke concrete opsporingsonderzoeken worden opgepakt. Eén van de door ons onderzochte korpsen maakt voor het maken van die keuze gebruik van bepaalde specifiek benoemde criteria die zijn vastgelegd in beleidsmatige programma's. In deze programma's is beschreven welke doelstellingen de organisatie nastreeft. In de zogenoemde preweeg-documenten[245] en onderzoeksvoorstellen dient te worden beargumenteerd hoe en waarom het onderhavige onderzoek een bijdrage levert aan de beleidsuitgangspunten. Er vinden periodiek overleggen plaats en de stuurploeg neemt daadwerkelijk beslissingen. Vaak liggen daar ook bepaalde strategische inzichten aan ten grondslag. Wij hebben vastgesteld dat in toenemende mate daadwerkelijk op een dergelijke wijze programmatisch wordt gestuurd. In de woorden van een respondent:

"*Waar we naar toe moeten (...) is het vooraf indienen van preweeg-documenten, projectvoorstellen, plannen van aanpak onderzoek opstarten. Die cyclus zit er nu in. Er komen geen onderzoeken uit de lucht vallen, bom, we gaan ergens beginnen. Dat*

[244] Zie voor de prioriteiten: Brief Minister van Veiligheid en Justitie, *Kamerstukken II*, 2010-11, 30880, nr. 237. Met betrekking tot de bestrijding van georganiseerde criminaliteit zijn de thema's mensenhandel, verdovende middelen, witwassen en zware milieucriminaliteit benoemd als prioriteit.

[245] Een preweeg-document (in politiejargon eenvoudigweg 'preweeg' genoemd) is een soort vooraankondiging van een op te starten opsporingsonderzoek. In een preweeg beargumenteren de opstellers (een RIO of de CIE) waarom het zinnig is om naar een bepaalde criminele groepering of een bepaald individu een onderzoek op te starten. Het onderzoek wat aan de preweeg vooraf gaat is vrij summier. De indiener beargumenteert waarom het goed zou zijn om een onderzoek in te stellen, maar gaat nog niet in op hoe dat vervolgens zou moeten. Indien het preweeg wordt goedgekeurd, kan er een uitgebreider onderzoeksvoorstel worden opgesteld waarin meer concreet de te voeren strategie wordt voorgesteld. Ook over onderzoeksvoorstellen moet de stuurploeg een beslissing nemen.

zijn de goede ontwikkelingen (…). Het wordt nu eigenlijk helemaal gestuurd. De stuurploeg bepaalt welk onderzoek er gaat gebeuren. Maar wat er gaat gebeuren, hangt natuurlijk af van de informatie die de stuurploeg krijgt. Daar vallen nog wel wat slagen in te maken. (…) Wat er moet gebeuren is dat er overzicht en inzicht moet komen. Daar staan alle boeken van vol, maar nou de praktijk." Interview analist CIE (F), april 2009.

Inmiddels wordt deze manier van werken door het betreffende korps toegepast op de meeste criminaliteitsgebieden. Het is een goed voorbeeld van hoe het element van sturing binnen IGP vorm kan krijgen.

Met betrekking tot bepaalde onderwerpen bleek het nemen van strategische beslissingen en het formuleren van beleid een zeer traag proces te zijn. Zo heeft het vier jaar geduurd voordat er sprake was van een programmatische sturing op één aandachtsgebied. Voor de andere aandachtsgebieden geldt dat de beleidsdoelstellingen na vijf jaar nog steeds niet vast staan. Daarnaast wordt er door de door ons onderzochte korpsen ook gewerkt met een lijst van subjecten die op de aandacht van het korps kunnen rekenen (een soort criminele top 100). Deze lijst is van groot belang, omdat de aanpak van de subjecten op die lijst de hoogste prioriteit zou moeten hebben. De subjecten van de top 100 zijn de subjecten waarop preweegvoorstellen moeten worden ingediend en concrete opsporingsonderzoeken en CIE-trajecten moeten worden opgestart. Het vaststellen van wie er op die lijst zou moeten komen te staan, is een proces dat bij het afsluiten van ons onderzoek al vier jaar in beslag had genomen. Het is vooralsnog zonder resultaat gebleven. Er werden werkgroepen ingesteld die hiervoor zouden moeten zorgen, maar deze werkgroepen werden vervolgens niet aan termijnen gehouden. Daarnaast kregen ze geen specifieke doelstellingen en veranderden ze vaak van samenstelling, waarmee de continuïteit niet werd gewaarborgd. Dit probleem speelt overigens niet alleen bij het vaststellen van een top 100: vrijwel alle onderwerpen die op een dergelijke wijze worden aangepakt, lijken hieronder te lijden. De beslissing om een top 100 vast te stellen is dus snel genomen, maar dat geldt kennelijk niet voor de uitwerking van de beslissing. Dit bemoeilijkt de verdere sturing op strategisch niveau.

De vraag die rijst, is wat de verklaring is voor de trage uitwerking van het strategische beleid. Wij noemen vier verklaringen. Allereerst is volgens sommige respondenten geen sprake van daadwerkelijke verantwoordelijkheid en de bijbehorende verantwoording voor leidinggevenden binnen de politieorganisatie in het algemeen en de RIO en CIE in het bijzonder. De constatering van een respondent dat "*politiemensen nog nooit een euro echt hebben hoeven te verdienen*" (runner CIE (A), maart 2007) is typerend voor de stellingen van gesprekspartners en respondenten die wij herhaaldelijk hebben vernomen. Leidinggevenden worden binnen de politie doorgaans niet gestimuleerd of beloond om projecten tot een daadwerkelijk goed einde te brengen (zie ook: Sales 2010: 323-331). Een tweede verklaring is het grote verloop onder de strategisch leidinggevenden. Vaak zitten leidinggevenden korter dan vijf jaar op hun positie. Dit komt de continuïteit die nodig is om veranderingsprocessen tot een goed einde te brengen niet ten goede. De belangrijkste, derde verklaring is volgens de respondenten echter dat strategische sturing in veel opzichten competenties vereist waarover de gemiddelde politieleidinggevende volgens hen niet zou beschikken. Veel leidinggevenden worden geworven uit de politieorganisatie zelf en beschikken over veel (relevante) recherche- of andere politie-ervaring. Maar een typische politieman heeft kenmerken en kwaliteiten die in bepaalde opzichten haaks staan op de eisen die nodig zijn voor (strategische) sturing

(zie onderdeel E van deze subsectie voor een verdere inhoudelijke behandeling van deze problematiek). Een recherchekundige drukt het als volgt uit.

"*Het wordt opgelegd: de standaarden waar je als professionele organisatie aan zou moeten voldoen. Dan moet je inderdaad voordat je wat gaat doen een plan van aanpak maken. En dan moet je over budgetten nadenken, uitzoeken, dan heb je handtekeningen nodig voordat je ergens aan begint. Maar politiemensen houden daar helemaal niet van. Die lezen (…) het liefst niet meer dan één A4-tje. Ze houden van actie. Ze houden niet van papier, ze houden niet van plannen, van notulen maken, van structuur aanbrengen. Ze houden niet van zich verantwoorden. Misschien ook wel omdat politiewerk vanuit vroeger een heel vrij beroep is geweest en dat ze nu steeds meer zich moeten verantwoorden. (…) Rapportjes tikken, formulieren invullen, daar houden ze niet van. Dat is met alles. Er is een soort papieren werkelijkheid bij de politie en die strookt helemaal niet met hoe het in de werkelijkheid echt is. Want in de werkelijkheid pakken ze het liefst nog die vrijheid zo goed en zo kwaad als het kan.*" Interview recherchekundige RIO (A), mei 2010.

De vierde verklaring is de afstand tussen de theoretische strategische besluitvorming en de praktijk op de werkvloer. Ten behoeve van een verantwoording naar de buitenwereld worden strategische programma's (zowel landelijk als regionaal) opgezet, maar volgens veel respondenten staat dit los van de dagelijkse praktijk. De politie is in dit opzicht in hoge mate een *verbal society*: "*het gesproken woord en de collegiale verhoudingen wegen vaak aanmerkelijk zwaarder dan de gedocumenteerde werkelijkheid*" (Boin, Van der Torre en 't Hart 2007: 325). Daarbij komt dat de strategische onderwerpen en producten nauwelijks de werkvloer bereiken. De medewerkers van de werkvloer hebben een grote afstand tot de strategische besluiten en inzichten, wat tot gevolg heeft dat veel van de beslissingen niet worden gedragen door de werkvloer. Het is een veelgehoorde klacht op de werkvloer. Het is echter de vraag in hoeverre het noodzakelijk is dat deze producten ook door de werkvloer worden gelezen en begrepen. Vanuit de stuurploegen wordt een kader geboden voor de verdere taakstelling en coördinatie. De werkvloer dient vervolgens het beleid uit te voeren en hoeft niet te worden meegenomen in de besluitvorming. Desalniettemin rijst de vraag in hoeverre de werkvloer (in ons onderzoek bestaande uit de CIE en de RIO) in staat is om het strategische beleid naast zich neer te leggen of, in het meest extreme geval, actief verzet te plegen tegen dat beleid. Dit is een aspect van de sturing van de dagelijkse politiepraktijk dat wij in subsectie 7.2.2 zullen behandelen.

B: Verschillen in zwacri-beleid

Een ander probleem dat wij op basis van onze observaties constateren, is het verschil in zwacri-beleid dat er tussen de verschillende korpsen bestaat. Een teamleider verwoordt dit als volgt.

"*ik ben echt verbaasd dat elke regio een eigen zwacri beleid heeft. Het is nu een rommeltje: de lokale driehoek komt bij elkaar en er wordt beleid ontwikkeld. Maar dit beleid staat haaks op het beleid ergens anders. We hebben een eenduidig beleid nodig. En dit moet vanuit een goede informatie-positie worden gerealiseerd. Ergens moet er gewoon een politiebrede (organisatie) komen waar de besluiten worden genomen. Nu doet iedereen maar wat. Zwacri beleid zou je (vanwege de aard van de*

materie) moeten beleggen op nationaal niveau, bijvoorbeeld bij de DNR." (Voormalig) medewerker AIVD (B), januari 2008.

De bestrijding van georganiseerde criminaliteit en terrorisme verloopt volgens de aangehaalde respondent niet efficiënt en effectief omdat er nog teveel verschil zit tussen het zwacri-beleid van de verschillende korpsen. Daarnaast blijkt uit wetenschappelijk onderzoek onder de Nederlandse korpschefs dat de korpschefs elk hun eigen visie hebben op de wijze waarop een politiekorps aangestuurd dient te worden (zie Boin et al. 2007). De korpschefs zijn zoekende naar de beste modaliteit, maar totdat hierin duidelijke keuzes zijn gemaakt "*blijft de politie kwetsbaar voor de bekende pendules in denkbeelden over beleid en sturing (…). De traditionele gretigheid waarmee allerlei trends en* management fads (cursief in oorspronkelijke tekst) *binnen de politie worden omarmd, versterken deze kwetsbaarheid*" (Boin et al. 2007: 325). Indien er geen eenduidige visie op beleid en sturing is, dan zal dit ook doorwerken in de inhoudelijke geformuleerde strategieën. De onduidelijkheid betekent in de praktijk voorts dat het middenkader van de leidinggevenden wordt belast met het daadwerkelijk uitwerken van het beleid. Zij bevinden zich in het spanningsveld tussen de kerntaken en het geformuleerde beleid van de korpschefs enerzijds en de taakopvattingen van de werkvloer anderzijds. Het gevolg is een kloof tussen beleid en uitvoering (zie Boin et al. 2007: 324-325).

C: De rol van de CIE bij beleidsvorming

Het bovenstaande geldt voor de politie in het algemeen. We zullen nu de CIE behandelen. De CIE is van oudsher een grotendeels autonome eenheid die veel van de werkzaamheden zelf kan bepalen en inrichten. Door middel van het implementeren van IGP proberen de korpsen aan die situatie een einde te maken. De CIE moet binnen het NIM meer dan voorheen een onderdeel uitmaken van het bredere opsporings- en intelligenceproces, en zal meer en beter moeten integreren in de bredere opsporingsorganisatie. Dit heeft belangrijke gevolgen voor de praktijk van het CIE-werk.

Zo verliest de CIE in belangrijke mate haar autonomie. Het is in theorie niet langer het hoofd CIE die bepaalt wat er gebeurt en wat de prioriteiten van de CIE zijn, maar de stuurgroep. Uit ons empirisch onderzoek is gebleken dat dit niet zonder slag of stoot plaatsvindt (zie ook subsectie 7.6.1). Zo worden bepaalde verantwoordelijkheden bij de CIE weggehaald en bij andere afdelingen geplaatst. Dit leidt tot de situatie dat de drie fasen van het CIE-proces (verzamelen, verwerken en verstrekken) niet langer allemaal bij de CIE worden neergelegd. De RIO's krijgen in toenemende mate een rol bij de verwerking van CIE-informatie en ook de verstrekking wordt door middel van autorisatiemodellen steeds meer van de CIE weggehaald (zie voor de ontwikkelingen op het gebied van verwerken en verstrekken respectievelijk secties 7.4 en 7.5). Wat voorheen exclusief tot de CIE-fase toebehoorde, wordt in toenemende mate door andere organisatieonderdelen (zoals de RIO) overgenomen. Overigens ziet het ernaar uit dat de CIE in de nog te implementeren nationale politie een onderdeel zal worden van de RIO. De rol van de CIE in de opsporing in het algemeen wordt van minder belang en daarmee vermindert ook de invloed van de CIE op het strategische besluitvormingsproces. Hierin zit een risico. De CIE is namelijk bij uitstek geschikt om snel zicht te krijgen in de relevante ontwikkelingen in het criminele milieu en kan als eerste zicht krijgen op nieuwe onderwerpen waarover strategische beslissingen genomen dienen te worden. Als de

CIE te ver wordt gemarginaliseerd ten opzichte van andere informatieafdelingen, bestaat het gevaar dat relevante inzichten niet worden meegenomen in de strategische beleidsvorming. Overigens is deze ontwikkeling deels ook het gevolg van de wijze waarop de CIE-en zelf jarenlang invulling hebben gegeven aan hun activiteiten. De nadruk heeft altijd al met name gelegen op het verzamelen van informatie, hetgeen ten koste is gegaan van bijvoorbeeld analysecapaciteit. Het feit dat de analyse van informatie nu wordt ingericht in RIO's is dan ook deels te wijten aan de eenzijdige invulling van de CIE-taak door de CIE-en zelf (zie ook subsectie 7.5.3).

D: De prestatieplicht

Op strategisch niveau wordt de politie geconfronteerd met een door de minister opgelegde prestatieplicht (zie: De Kleuver 2007).[246] Deze kwantitatieve prestatiesturing staat in principe los van IGP. Het kan echter wel een rol vervullen binnen IGP, de CIE en de RIO. Zo kan bijvoorbeeld worden vastgesteld dat er een vastgesteld aantal informatieproducten dient te worden opgeleverd of dat de CIE een bepaalde hoeveelheid processen-verbaal dient te verstrekken. Een projectmedewerker IGP verwoordt dit als volgt.

"*Bij de politie wordt de sturing met name op een prestatie- en beheersgerichte manier vormgegeven. Het gaat om zichtbare resultaten. Intelligence is geen zichtbaar resultaat en hier wordt niet op gestuurd. Voorkomen van criminaliteit kun je niet meten en dit telt dus niet mee bij de prestatiegerichte organisatie."* Interview projectmedewerker IGP (A), februari 2008.

Wij zijn het niet helemaal eens met deze respondent. Intelligence kan wel degelijk een *zichtbaar* resultaat opleveren. Immers, er worden analyseproducten opgeleverd, er wordt centraal beleid vastgesteld *et cetera*. Dit is allemaal zichtbaar. Daarnaast hebben vrijwel alle politiële interventies met betrekking tot (georganiseerde) criminaliteit en terrorisme invloed op 'het milieu', en het is denkbaar dat er een verandering optreedt in (de perceptie van) criminaliteit of veiligheid in het algemeen, of dat er bijvoorbeeld onrust in het criminele milieu ontstaat. Ook dit is zichtbaar. Het is echter zeer moeilijk *meetbaar* in de zin dat er nauwelijks een causaal verband valt vast te stellen tussen zichtbare ontwikkelingen (een daling van criminaliteit) en de implementatie van intelligence. Het resultaat van intelligence valt dus niet te meten, hetgeen overigens geldt voor het meten van resultaten van de politie in het algemeen. Dit specifieke probleem van het meten van politiecijfers laten wij verder buiten beschouwing.

Een ander onderdeel van de prestatieplicht is dat de vorm van bepaalde producten dwingend worden voorgeschreven. Producten dienen in politiejargon 'eenvoudig' en 'stapelbaar' te zijn, dat wil zeggen dat ze op elkaar moeten lijken zodat ze gemakkelijk gecombineerd en vergeleken kunnen worden. Ook hier lijkt echter sprake te zijn van een papieren werkelijkheid ten opzichte van de beleving van de werkelijkheid door de medewerkers op de werkvloer. Deze papieren werkelijkheid heeft vaak weinig meer te maken met de daadwerkelijke georganiseerde criminaliteit of terrorisme. In de woorden van een analist:

[246] Dit is het gevolg van de theorie van het *New Public Management* en de toegenomen nadruk op het managen van de politie (in het Engels *managerialism* genoemd: zie ook Jones en Newburn 2005: 740 e.v.).

"*Men heeft geprobeerd om met een visie en beleid te komen, maar het is zeer verwarrend voor de mensen van de werkvloer. Op papier ziet het er allemaal mooi uit en zijn er prachtig mooie structuren beschreven, maar in de praktijk klopt het niet. De criminaliteit is anders, dat is niet opgedeeld in aandachtsgebieden. Je hebt polici-criminelen die alles doen, een cocaïnelijn, afpersing, overval en noem maar op. Je apart richten op de aandachtsgebieden werkt dan niet omdat je dan een gefragmenteerd beeld van de werkelijkheid krijgt. De strategie moet niet alleen maar worden gericht op een aandachtsgebied. Helaas is de kennis en kunde er niet om alles goed te interpreteren.*" Interview analist CIE (G), maart 2011.

De papieren werkelijkheid betreft de verantwoording naar bijvoorbeeld de stuurgroep. De producten worden plichtmatig geproduceerd, maar worden gezien als vervelende taken die zo snel mogelijk moeten worden afgehandeld. Er wordt weinig tijd in gestoken om ze kwalitatief op een hoog niveau te brengen. Een voorbeeld hiervan zijn de CSV-beschrijvingen die jaarlijks door de korpsen moeten worden ingeleverd.[247] Wij constateren dat tijdens het veldwerkonderzoek één maand voordat de deadline verstrijkt er snel mensen vrij worden gemaakt voor het produceren van CSV-beschrijvingen. Dat moet allemaal erg snel en alleen maar omdat het verplicht is gesteld. De analisten die worden belast met het maken van de CSV-beschrijvingen, beklagen zich herhaaldelijk over het feit dat de CSV's het hele jaar door niet stelselmatig worden bijgehouden: indien dit wel zo zou zijn, dan zou dat immers veel werk aan het einde van het jaar schelen. De verklaring die zij hiervoor geven was dat het eenvoudigweg wordt gezien als een onbelangrijke klus. De vraag is voorts of de CSV-beschrijvingen daadwerkelijk inzicht *kunnen* geven in de criminele werkelijkheid. De kwaliteit hangt af van de invulling, en de invulling laat te wensen over (zie ook: Huisman et al. 2011).

E: De waan van de dag

Een terugkerende omschrijving van de sturing van de CIE en de RIO door respondenten is de 'waan van de dag'. Er vindt eigenlijk nauwelijks proactieve, langetermijn-sturing plaats: de leidinggevenden reageren met name op gebeurtenissen. Een teamleider zegt hierover het volgende.

"*Hier bij de RIO is nog geen IGP. Het is hier veel te veel van de hak op de tak en ad-hoc. Mensen weten niet waar ze het over hebben. Men weet niet waar relevante informatie ligt. Neem nou zaak X (…): er wordt erg lang doorgepraat op basis van een krantenbericht. Er is hier gewoon een super klein referentiekader. Waar dat vandaan komt, weet ik niet.*" Teamleider RIO (A), januari 2008.

Het waan-van-de-dag-denken speelt, anno 2012, zowel bij de CIE-en als de RIO. Een runner merkt het volgende op.

"*Ja, het is (waan van de dag), een afdeling waar runners rondlopen die helemaal zelf kunnen bepalen waar ze mee bezig zijn en zelf hun bronnen zoeken. Incidenteel krijgen ze bronnen aangereikt omdat dit actueel is in een bepaald onderzoek. Men*

[247] Een CSV-beschrijving is een weergave van een crimineel netwerk. Het geeft inzicht in wie met wie samenwerkt, hoe de groepering is gestructureerd, hoeveel geld er wordt witgewassen *et cetera*. De regionale politiekorpsen zijn verplicht om deze CSV-beschrijvingen jaarlijks bij het KLPD in te leveren, zodat die politiedienst overzichten kan genereren over de CSV's die in Nederland actief zijn.

moet daar een informatiepositie verkrijgen. Er is geen idee van 'we willen een bepaald onderwerp eens goed in beeld krijgen'. Dat begint zo langzamerhand wel een beetje te komen omdat de analisten die er nu zitten ook meer van die structuur zijn en op eigen initiatief eigenhandig een structuur aan proberen te brengen, maar het is nog geen onderdeel van het werkproces. (…) Dat doet de werkvloer zelf. En op zich is dat wel een prettige ontwikkeling, maar het valt nog steeds onder de waan van de dag. Want het is nog steeds de analist zelf die naar eigen goeddunken werkt." Interview runner CIE (D), maart 2011.

De meeste leidinggevenden zijn afkomstig uit de politieorganisatie zelf. Ze zijn gevormd door de speciale omstandigheden die het politiewerk op straat kenmerken. Kort samengevat vereist het dagelijkse politiewerk (surveillance en noodhulpverlening) snelle beslissingen. Wanneer een politieman als eerste bij een verkeersongeval ter plaatse is, dan wordt van hem verwacht dat hij direct handelt. Er zijn weliswaar vaak verschillende protocollen waar hij aan moet voldoen, maar in de praktijk komt het erop neer dat hij direct beslissingen moet nemen en handelen; de protocollen en andere regels komen later wel. Een politieman op straat doet en handelt, hij reageert dus op datgene wat om hem heen gebeurt. Dit vormt de kwaliteiten waar de politieman aan moet voldoen: praktisch en pragmatisch. Met andere woorden: iemand die reageert. De typische politieman voelt zich dus op zijn gemak in het geval van een crisis of van chaos. Een recherchekundige bracht dit als volgt onder woorden.

"*En dat vindt de organisatie ook wel fijn volgens mij. (De) leidinggevenden op informatiegebied (vinden) de chaos ook wel prettig (…) omdat ze het beste in chaos functioneren. (…) Een stukje onbekendheid met wat er gaat gebeuren, dat is voor een bepaald type mens aantrekkelijk.*" Interview recherchekundige RIO (B), maart 2011.

Leidinggeven vereist echter ook andere kwaliteiten, niet in de laatste plaats met betrekking tot het managen van een afdeling. Leidinggevenden zijn doorgaans verantwoordelijk voor personeel en budgetten, en vormen het beleidskader van de organisatie. Het maken van beleid is een lange-termijn-bezigheid. Dit beleidskader kent een bijzonder verregaande bureaucratie, met veel vergaderingen en complexe en langdurige besluitvorming. Het belang van een lange-termijn-planning geldt in toenemende mate ook voor operationele werkzaamheden, met name voor leidinggeven binnen IGP. IGP eist van leidinggevenden dat zij binnen het operationele proces steeds meer beleidsmatig gaan denken. Eenvoudig geformuleerd ligt bij IGP de nadruk op de stelregel 'eerst denken, en dan doen'. In het recherchewerk in het algemeen en het werk van de CIE in het bijzonder is er overigens meestal voldoende tijd om na te denken. Slechts in uitzonderingsgevallen is er een operationele noodzaak waardoor er direct snel moet worden gehandeld. Een RIO-analist verwoordt dit als volgt.

"*(…) In deze organisatie waar wij zitten ligt het accent veel meer op eerst denken en analyseren, eerst kijken en opties bekijken, inschatten wat de risico's en scenario's zijn. Wat kunnen we verwachten, welke belangen spelen er? Daar zit een veel groter denkproces achter. Dat doe-proces is hier eigenlijk niet. Want zodra er wat gedaan moet worden, wordt het overgedragen aan tactiek, die gaan het dan doen. Wij zitten hier in het denkproces. Maar alle leidinggevenden zijn gewoon doeners.*" Interview analist RIO (B), mei 2010.

Wij constateren dat een deel van de leidinggevenden in de politiepraktijk doorgaans niet over de juiste kwaliteiten lijken te beschikken die nodig zijn voor de lange-termijn-sturing die binnen IGP wordt vereist. Deze leidinggevenden zijn nooit geselecteerd op de kwaliteiten die nodig zijn om binnen een bureaucratische organisatie leiding te geven. Zij hebben zich ontwikkeld in een waan-van-de-dag-organisatie, en die *mindset* passen ze grotendeels ook nog toe in het recherchewerk. De beslissingen worden ad hoc en op korte termijn genomen, en er zijn weinig leidinggevenden die oog hebben voor de lange termijn. Het leidinggeven in een bureaucratie en het leidinggeven aan operationele processen binnen IGP vereisen echter zoals gezegd andere kwaliteiten. Een recherchekundige van de RIO zei er het volgende over.

"*(…) Als je hier in een recherchetak zit wat eigenlijk gewoon kantoorwerk is en wat veel meer intellectueel is dan praktisch, dagelijks zit je achter een bureau op een computer te werken en vergaderingen te houden. Dat is een heel andere mindset dan op straat. Maar je merkt wel dat mensen die van de straat omhoog zijn gekomen en hier terecht zijn gekomen als leidinggevende niet over de capaciteiten beschikken om hier leiding te geven.* ***(…)*** *Wat er het meeste in zit is 'actie, actie, actie' en niet denken maar doen."* Interview recherchekundige RIO (A), mei 2010.

De implementatie van het concept van IGP vereist op zichzelf veel planning. Ook daar stellen wij vast dat er in de praktijk weinig sprake van is. Het is daarbij opvallend dat voor de meeste functieomschrijvingen voor het leidinggevende kader aan de ene kant de eis van een executieve *achtergrond* wordt gesteld en aan de andere kant een academisch *werk- en denkniveau*. Er wordt voor deze hogere leidinggevende posities kennelijk nog steeds veel nadruk gelegd op de operationele component van het werk. Diegenen die in aanmerking komen voor een leidinggevende functie zijn dan ook doorgaans politiemensen met een 'blauwe' achtergrond. Er wordt in de praktijk nog te weinig rekening gehouden met het feit dat de aard van de werkzaamheden eigenschappen vereisen die niet goed te rijmen zijn met een executieve achtergrond en daar in sommige gevallen zelfs haaks op staan. De functies voor leidinggevenden zijn doorgaans veel minder operationeel dan men in de functieomschrijvingen doet voorkomen: leidinggeven bestaat bijvoorbeeld voor een groot deel ook uit functioneringsgesprekken en het zorg-dragen voor de faciliteiten waarmee de medewerkers hun werk kunnen doen. Daarnaast behoeft de operationele ervaring die het politiewerk vereist niet altijd direct bij de leidinggevende zelf te liggen. Het is goed denkbaar dat de ervaring wordt gezocht bij de medewerkers die een adviserende rol kunnen vervullen. Wij hebben tijdens ons veldwerk geconstateerd dat hiervan in de praktijk bijna geen sprake is: vrijwel alle leidinggevenden op de afdelingen waar wij onderzoek hebben gedaan, hebben een executieve achtergrond. Hierbij moet wel de kanttekening worden geplaatst dat met name voor functies in de korpsleiding geldt dat hiervoor steeds vaker ook externen worden aangenomen. Wellicht dat het slechts een kwestie van tijd is voordat deze ontwikkeling ook bij de rechercheonderdelen plaatsvindt.

In het verlengde van het voorgaande: uit onze observaties blijkt voorts dat leidinggevenden die op beleidsniveau dienden te acteren, erg veel bezig waren met operationele zaken. Ze konden het operationele werk maar moeilijk loslaten. De leidinggevenden gaven zelf ook aan dat de aansturing van operationele activiteiten hun voorkeur heeft boven het aansturen van meer beleidsmatige zaken: "*ik heb*

eigenlijk niet zoveel met managen" (hoofd CIE (B), februari 2009). Wij constateren op basis van onze observaties dat leidinggevenden die een afdeling van ongeveer 100 man onder zich hebben, zich inhoudelijk bemoeien met de details van opsporingsonderzoeken en inlichtingentrajecten.[248] Ze passeren de teamleiders en nemen beslissingen in concrete opsporings- en inlichtingenonderzoeken (zoals hoe een verhoorplan in zaak X eruit moet zien of op welke verdachte uit netwerk Y een telefoontap moet worden geplaatst). Dit speelt zowel bij de informatieafdelingen als bij de CIE. Bij de CIE zijn er teamchefs en hogere leidinggevenden die zelf betrokken zijn bij het runnen van informanten. In het geval van de teamchefs komt dit doorgaans vanwege capaciteitsgebrek: indien er slechts één runner in dienst is en een informant neemt contact op die aangeeft dat hij dringend zijn runners wil spreken, dan kan een teamchef met de runner mee gaan. Wij hebben echter ook vernomen dat een hoofd CIE en diens plaatsvervanger incidenteel bepaalde informanten zelf spreken omdat het informanten van 'een bepaald niveau' zouden zijn. De formele reden voor deze gang van zaken is dat omdat het hoofd CIE verantwoordelijk is voor het gehele CIE-traject, hij in speciale gevallen volgens de gegeven argumentatie het gesprek met de informant dient te voeren. Enkele respondenten geven tijdens informele gesprekken aan de koffietafel hieromtrent echter aan dat zij van mening zijn dat het hoofd CIE en diens plaatsvervanger zelf de praktijk van het runnen moeilijk kunnen loslaten, en dat ze het eigenlijk veel te leuk vinden om met 'zware' informanten te spreken. Verschillende leidinggevenden vertellen ons dit tijdens koffiegesprekken zelf ook. Vanwege de bindingstermijnen voor runners (één keer vier jaar met mogelijk twee keer twee jaar verlenging) moest een aantal op een bepaald moment stoppen met het runnersvak. Een deel daarvan is leidinggevende geworden. Zij geven aan dat ze dat werk wel missen en vanuit dat gevoel vrij gretig zijn om met de runners mee de straat op te gaan.

Net als bij de CIE constateren wij met betrekking tot de RIO dat de leidinggevenden met name zijn gericht op het operationele aspect van het werk. Zo zijn er leidinggevenden die zich met de inhoud van inwinplannen bemoeien en worden adviezen en analyses op het laatste moment door de leidinggevenden aangepast omdat zij over de meest relevante en recente informatie zouden beschikken.

De grote betrokkenheid bij operationele activiteiten wordt door een aantal medewerkers overigens ook erg gewaardeerd: "*bij hem gaat het tenminste over de inhoud*" (interview analist RIO (D), maart 2009). Zij geven aan dat ze in de loop van hun carrière zijn overspoeld met managementinformatie waar ze naar eigen zeggen geen boodschap aan hebben: "*we komen om in de procesbeschrijvingen, ABRIO documenten en noem maar op. Ik wil gewoon mijn werk doen.*" (interview analist CIE (C), maart 2009). Deze medewerkers zijn van mening dat de leidinggevenden die zich met de operationele activiteiten bemoeien, in ieder geval snelle en voor hun werk relevante beslissingen nemen.[249] Aardema (2007) onderscheidt in dit opzicht een onderstroom en een bovenstroom binnen de politie, en leidinggevenden acteren niet zelden in beide stromen tegelijkertijd. De onderstroom is het 'het echte politiewerk', en betreft het leidinggeven aan de operationele werkzaamheden van de politie. De

[248] In veel regio's is de CIE overigens veel kleiner en bestaat gemiddeld uit een CIE-chef, tien runners, twee administratieve medewerkers en een operationele analist.

[249] Leidinggevenden dienen ook tegemoet te komen aan de kenmerken van de *ingroup* om succesvol te zijn (Haslam en Platow 2001: 221). Een bepaalde mate van operationele affiniteit en de bijbehorende *mindset* kan dus geen kwaad. Het wordt echter problematisch wanneer leidinggevenden de andere noodzakelijke kwaliteiten missen en alleen maar operationeel zijn ingesteld. Dit laatste zijn wij in de praktijk vaak tegengekomen.

bovenstroom is het leidinggeven aan de beleidsmatige kant van het politiewerk (Aardema 2007: 9). Het is overigens zeer wel mogelijk dat een hoge, strategische leidinggevende zoals een korpschef leiding geeft in de onderstroom, bijvoorbeeld wanneer er interactie is met wijkteamchefs of andere operationele medewerkers. Dat zo'n leidinggevende dat doet, kan dus legitiem en noodzakelijk zijn en het kan helpen bij de acceptatie van de leidinggevende in kwestie. Wij stellen echter vast dat het problematisch wordt wanneer de sturing in de bovenstroom wordt uitgevoerd op basis van de regels en normen (de mores) die gelden in de onderstroom. Volgens de respondenten en onze observaties lijkt hier niet zelden sprake van te zijn. Het verschil tussen de boven- en onderstroom zullen we in subsectie 7.2.2 ook nog tegenkomen.

Al met al concluderen wij dat het strategische beleid niet vanzelfsprekend door de medewerkers op de werkvloer wordt geaccepteerd. Dit is echter niet alleen een onderwerp van strategische sturing, maar het raakt uiteindelijk ook de operationele en tactische sturing.

7.2.2 Dilemma's van operationele en tactische sturing

In deze subsectie onderzoeken wij de wijze waarop deze operationele en tactische sturing in de CIE- en RIO-praktijk vorm krijgt. Wij behandelen als eerste (A) de belangrijkste theoretische inzichten met betrekking tot de barrières tegen de sturing van het politiewerk. Het gaat allereerst om de *street-level bureaucracy*. Wij bezien in hoeverre hier binnen de CIE sprake van is en op welke wijze de operationele en tactische sturing wordt belemmerd. De tweede barrière tegen sturing is het traditionele conflict tussen twee subculturen die sturing bemoeilijkt. Het gaat dan om de zogenoemde *street-cop culture* en de *management cop culture*. Daarna (B) behandelen wij in hoeverre wij deze twee barrières in de praktijk zijn tegengekomen. We sluiten af met (C) de sturing van de zij-instromers en analisten in de praktijk. Deze groep wordt apart behandeld omdat zij binnen IGP een cruciale rol vervullen en in vele gevallen afwijken van de traditionele CIE-medewerkers.

A: Theoretische verklaringen voor de barrières tegen sturing

De sturing van het dagelijkse politiewerk in het algemeen is in de wetenschap al vaak onderzocht (zie Lipsky 1980; Van der Vijver en Terpstra 2007). De algemene bevindingen zijn dat de politie erg lastig te sturen is, en dat dit te maken heeft met de structuur van de politie. Het zou namelijk gaan om een *street-level bureaucracy*, waarbij de medewerkers die formeel het laagste in de hiërarchie staan feitelijk de meeste vrijheid hebben om de werkzaamheden naar eigen inzicht in te vullen (zie Lipsky 1980; Van der Vijver en Terpstra 2007: 367).

Naast de *street-level bureaucracy* is er binnen de politie ook sprake van twee politiële subculturen die tegenover elkaar lijken te staan: de cultuur van de uitvoerenden (*street cop culture*) en de cultuur van de leidinggevenden (*management cop culture*) (Reuss-Ianni en Ianni 1983; Van der Vijver en Terpstra 2007: 368). Een op hoofdlijnen vergelijkbare benadering van deze twee subculturen is het onderscheid tussen de bovenstroom en de onderstroom zoals aangebracht door Aardema (2007, zie subsectie 7.2.1).[250] Deze gescheiden subculturen (stromen) belemmeren de sturing

[250] Aardema geeft aan dat het onderscheid tussen de bovenstroom en de onderstroom niet samenvalt met het onderscheid tussen top en werkvloer, en dat leidinggevenden in beide stromen actief kunnen zijn. Zijn bevindingen liggen echter verder in de lijn met de *street-level bureaucracy* en de cultuur-benadering van Ianni.

van het politiewerk. In essentie streven beide subculturen hetzelfde na: veiligheid en criminaliteitsbestrijding. Maar over de wijze waarop dat dient te worden gerealiseerd, bestaan tussen de *street-level cops* en de *management cops* verschillende opvattingen. Dit kan leiden tot conflicten tussen de subculturen: "(…) *de voortdurende drang van bovenstromen naar regeling/beheersing/verandering/vernieuwing (wordt) niet altijd geapprecieerd in onderstromen* (…). *Tegen de (boven)stroom in blijven mensen 'gewoon hun werk doen'*" (Aardema 2007: 16). Indien de subcultuur van de uitvoerenden in conflict komt met die van de leidinggevenden, dan zal het voor de laatsten erg moeilijk worden om de uitvoerenden te sturen. Deze beide barrières tegen sturing (de *streetlevel bureaucracy* en de gescheiden subculturen) zijn niet strikt van elkaar gescheiden. Conflicten tussen beide subculturen kunnen bijvoorbeeld voortkomen uit pogingen van de management subcultuur om de discretionaire ruimte van de uitvoerende medewerkers te beperken. Wij behandelen deze barrières dan ook gezamenlijk.

B: De barrières in de praktijk

Respondenten die in het leidinggevende kader functioneren (de *management cops*) geven aan dat de runners van de CIE doorgaans zeer lastig aan te sturen zijn. Zo wordt door diverse medewerkers gesproken van een leger waarin iedereen een generaal is (een Mexicaans leger): medewerkers bepalen grotendeels zelf wel wat ze doen en hoe ze een dag indelen. De runners van de CIE hebben een bijzonder grote discretionaire ruimte waarbinnen ze zelf invullen wat ze tijdens het werk (zullen gaan) doen. Veel van hun werkzaamheden vinden op straat plaats en er zijn geen leidinggevenden bij betrokken die daadwerkelijk zicht hebben op de activiteiten van de runner. In bepaalde gevallen worden pogingen tot sturing expliciet door runners tegengewerkt en bekritiseerd (voor zover wij dit kunnen beoordelen, betreft dit een minderheid van de runners). Opvallend is dat respondenten aangeven dat zij zelf geen moeite hebben met meer sturing, maar dat dit niet geldt voor collega's. In de woorden van een runner wordt dit als volgt geformuleerd:

"*De vrijheid zit wat mij betreft in hoe je een informant benadert. Dat is mijn expertise. Maar wie we moeten benaderen en waarom, daar mag best wat meer op worden gestuurd. Er zijn ook collega's die aangeven dat ze de mate van sturing nu prima vinden. Het moet echt niet meer worden, want dat tast de vrijheid aan.*" Interview runner CIE (D), maart 2011.

Een belangrijke vraag die nu rijst is hoe binnen IGP wordt geprobeerd om in de praktijk daadwerkelijk te sturen. De belangrijkste wijze waarop dit binnen IGP wordt geprobeerd, is het systeem van briefing en debriefing. De bedoeling van dit systeem is kort gezegd dat er gericht opdrachten worden gegeven en dat deze periodiek met de medewerkers worden doorgesproken (IOOV 2006: 51; Den Hengst-Bruggeling 2010: 18). Daarna vindt er een terugkoppeling door de betreffende medewerker plaats en wordt bekeken in hoeverre hij aan de opdracht uit de briefing heeft voldaan (de debriefing). Dit is de theorie van IGP. De vraag is echter in hoeverre dit in de praktijk wordt toegepast.

Uit onze observaties en de sociale gesprekken blijkt dat er weliswaar wordt gebriefd en gedebriefd, maar dit gebeurt doorgaans weinig gestructureerd. Runners bepalen over het algemeen zelf wat ze aan de informant vragen, en worden soms

gevoed met input van een analist of andere runners. Dit laatste is echter niet zelden afhankelijk van de runner zelf, en volgt dus niet uit een briefing.

In welke mate er een briefing en debriefing plaatsvindt, hangt in belangrijke mate af van de teamleider. Sommige teamleiders briefen en debriefen relatief vaak (een paar keer per week), andere teamleiders briefen bijna nooit. De teamleiders die het meeste briefen en debriefen, zijn overigens de jonge(re) leidinggevenden die geen runnerservaring hebben. Zij proberen door middel van briefen en debriefen wel te sturen, maar vanwege hun achtergrond krijgen zij juist erg veel weerstand.

Een tekortkoming van de briefings die wel plaatsvinden is dat onvoldoende duidelijk wordt waarom bepaalde informatie nodig is. De runners kunnen de noodzaak van de informatie voor het bredere analyse- en besluitvormingsproces niet goed inschatten (zie ook: Den Hengst-Bruggeling 2010: 32). Indien de nut en noodzaak van informatie niet duidelijk is, zullen de runners ook niet snel geneigd zijn om lang bij de aangegeven informatiebehoefte stil te staan. Hier kan dus nog behoorlijk wat worden verbeterd: een runner die weet waarom hij bepaalde vragen aan een informant moet stellen en dus bewust is van zijn concrete toegevoegde waarde in het bredere inlichtingen- en opsporingsproces, zal sneller geneigd zijn om deze vragen ook daadwerkelijk te stellen. Een runner die voordat hij op gesprek gaat een lijstje met vragen mee krijgt zonder dat hij weet waarom die vragen gesteld moeten worden, zal sneller geneigd zijn om de vragen als niet relevant te beoordelen en zijn eigen vragen gaan stellen. Volgens sommige respondenten zou het ook helpen als het voldoen aan concrete inwinplannen een onderdeel wordt van de formele beoordeling van de runners. Hieruit maken wij op dat dit in de praktijk kennelijk niet het geval is, hetgeen door respondenten tijdens de interviews wordt bevestigd. Kennelijk wordt één van de belangrijkste sturingsinstrumenten, te weten het functioneringsgesprek, niet aangewend om tot een daadwerkelijke operationele sturing te komen.

Debriefing vindt meer plaats dan briefing. Na een gesprek met een informant, bespreken de runners het gesprek meestal (kort) met de teamleider. Indien het heel gevoelige informatie betreft of de informatie vereist een extra actie van de politie (zoals de inzet van een observatieteam), worden de gesprekken met het hoofd CIE doorgesproken. Ons is ook gebleken dat er wekelijkse overleggen plaatsvinden tussen het hoofd, diens plaatsvervanger, de officier van justitie en de teamleiders waarin de operationele ontwikkelingen worden doorgenomen. Op deze manier blijft de leiding geïnformeerd over de operationele ontwikkelingen binnen de CIE. Van een vraaggestuurd werkproces is echter geen sprake, gezien het feit dat er nauwelijks wordt gebriefd. Echter, volgens de respondenten vindt in dit overleg in toenemende mate een vorm van briefing plaats, waarbij de aanwezigen onderling afspraken maken over te benaderen informanten en welke onderwerpen van belang zijn. Hiermee lijkt het CIE-proces in toenemende mate vraaggestuurd te worden. Ten tijde van ons onderzoek was dit echter lange tijd geen structureel onderdeel van het werkproces: pas aan het einde van ons onderzoek werd het een terugkerend overleg met een vaste structuur. En voor de concrete briefing van de runners geldt nog steeds de bovenstaande conclusie: de wijze waarop dit plaatsvindt, hangt sterk af van de betreffende teamleider.

Op het moment dat leidinggevenden daadwerkelijk inhoudelijk gaan sturen, kan er frictie met de runners optreden. Wij constateren dat hier in de praktijk soms inderdaad sprake van is. In sommige gevallen zijn de teamleiders zelf geen runners geweest, hetgeen vaak wordt aangehaald als kritiek: de leidinggevende in kwestie zou geen verstand hebben van runnen en moet niet denken dat hij in staat is om te

begrijpen wat het runnerswerk inhoudt, laat staan dat hij daar sturing aan kan geven. Dit maakt dat de runners minder snel geneigd lijken te zijn om een bepaalde aansturing te accepteren, zeker daar waar het de uitvoering van de dagelijkse werkzaamheden betreft. Het gaat hier echter met name om de oudere CIE-medewerkers die er al heel wat dienstjaren op hebben zitten. Deze categorie runners verzet zich het meeste tegen alle veranderingen binnen de CIE, en dus ook tegen de toenemende sturing. Zij roemen de vrijheid van het runnersvak en zien meer sturing als een aantasting van deze vrijheid. Het leidt dan tot een strijd tussen de leidinggevenden (de *management cops*) en deze groep medewerkers van de werkvloer (*street-level cops*). Dit is een voorbeeld van de hierboven genoemde cultuurstrijd met als inzet de discretionaire ruimte van de medewerkers van de werkvloer, hetgeen weer een voorbeeld is van de *street-level bureaucracy*. Vanwege het natuurlijke verloop van CIE-medewerkers zal het verzet van de oudere runners steeds minder voorkomen.

C: Sturing van zij-instromers en analisten

In alle paradoxaliteit observeren wij echter ook dat een groot deel van de respondenten klaagden over een *gebrek* aan sturing. Zij verzetten zich dus helemaal niet tegen sturing, maar willen juist dat er meer wordt gestuurd. En zij verwijten de leidinggevenden dat zij veel te veel terugvallen op de kwaliteiten die 'op straat' waardevol zijn, maar die doorgaans niet bijdragen aan effectieve sturing van de werkzaamheden van het personeel en leiderschap. Hier speelt hetzelfde probleem als wij eerder bij de strategische sturing signaleerden: de leiding neemt nauwelijks lange-termijn-beslissingen, maar laat zich leiden door de waan van de dag. Dit leidt bij een deel van de medewerkers tot frustratie:

"*Maar alle leidinggevenden zijn gewoon doeners. En als er een groot SGBO*[251] *is, duiken alle leidinggevenden op de operationaliteit. En ze gaan niet zitten en met een meer helikopterview kijken naar wat er aan de hand is, wat wordt er van ons verwacht, wat voor een plan kunnen we maken.*" Interview recherchekundige RIO (A), mei 2010.

Bij de tactische en operationele sturing zien wij duidelijk een strijd tussen twee subculturen, waarbij de discretionaire ruimte niet de inzet is, maar waarbij het juist gaat om een door de werkvloer ervaren overdaad aan vrijheid. Dit plaatst de leidinggevenden in een lastige positie: veel sturing leidt tot een conflict met het ene deel van de werkvloer, en weinig sturing leidt weer tot een conflict met het andere deel van de werkvloer. Het zijn overigens met name de hoger opgeleide zij-instromers die juist meer sturing en betrokkenheid van het leidinggevende kader wensen. De dilemma's zoals wij hiervoor beschreven zullen volgens ons alleen maar toenemen naarmate er meer zij-instromers bij de politie komen. Dit hangt overigens ook mede af van het (opleidings- en scholings)niveau van de niet-zij-instromers die op leidinggevende posities terechtkomen.[252]

Ook de analisten lijken over een zekere discretionaire ruimte te beschikken waarin ze zelf de werkzaamheden kunnen bepalen. In sommige gevallen maken ze op een vergelijkbare wijze als de runners gebruik van deze ruimte. Deze ruimte is echter

[251] SGBO staat voor Staf Grootschalig en Bijzonder Optreden. Dit is een hiërarchisch sturingsmodel dat bij calamiteiten zoals een op handen zijnde terroristische aanslag wordt gebruikt.

[252] Overigens willen wij hier niet mee suggereren dat een hogere opleiding een betere leidinggevende van iemand maakt

wel veel kleiner dan die van de runners, zeker daar waar het de analisten van de RIO betreft. Maar net als bij de runners is er bij de analisten een mogelijk probleem met de daadwerkelijke aansturing. Een teamleider verwoordt het als volgt.

"(…) *kreeg de opdracht om een* overallbeeld *te maken. We vroegen gewoon om een opzetje (*van een analyse, opmerking auteur*). De analisten weigerden gewoon. "Nee, dit doen wij niet. We moeten een duidelijke opdracht hebben, anders doen we het niet". Het enige wat we wilden was een opzetje zodat we met z'n allen konden kijken wat er mogelijk was. Maar nee hoor, op de opleiding hadden ze geleerd dat ze zo duidelijk mogelijk geformuleerde opdrachten moesten krijgen*." Interview teamleider CIE (D), november 2009.

De sturingsproblemen met de analisten en de zij-instromers zien doorgaans op de wijze waarop de werkzaamheden werden uitgevoerd en de inhoudelijke presentatie van de analyseresultaten. We zullen hier in sectie 7.5 dieper op in gaan. Hier volstaan wij met de constatering dat veel leidinggevenden niet goed lijken te weten wat ze met deze medewerkers aan moeten. Diverse respondenten merken op dat er een groot verschil zit tussen de zij-instromers en de door de wol geverfde politiemensen: zij-instromers worden gezien als 'denkers' en politiemensen als 'doeners'. Hier lijkt met name een proces van labelen en sociale categorisatie plaats te vinden (zie voor een inhoudelijke behandeling van deze fenomenen subsectie 7.5.3). Zij-instromers worden vaak automatisch in de categorie van denkers geplaatst en krijgen standaard het verwijt dat ze alleen maar over theoretische kennis beschikken. Door de traditionele politiemedewerkers (onder wie de leidinggevenden) wordt niet zelden getwijfeld aan de toegevoegde waarde van deze kennis voor de operationele werkzaamheden van (met name) de CIE.

De zij-instromers en de analisten blijken voorts voor veel leidinggevenden vanwege hun specialistische kennis erg lastig te sturen. Dit leidt in de praktijk enkele malen tot openlijke conflicten. Meestal wordt het openlijke conflict echter gemeden en lijken de leidinggevenden de bevindingen van de analisten en de zij-instromers eenvoudig naast zich neer te leggen en niet te gebruiken bij de besluitvorming. Wij krijgen de indruk dat er op bepaalde momenten een soort stil conflict wordt uitgevochten tussen de analisten en zij-instromers enerzijds en de leiding en traditionele medewerkers anderzijds. Zo is er periodiek sprake van een soort uitbraak van frustraties die wij op de werkvloer al een lange tijd hebben zien aankomen, maar waarvan het ons toch altijd weer verbaast hoe lang het duurt voordat het daadwerkelijk tot een uitbarsting komt. Wij hebben als onderzoeker echter nauwelijks inzicht in deze stille conflicten en zullen de behandeling van dit onderwerp hier dan ook staken.

7.2.3 Tussenconclusies

Met betrekking tot de strategische, tactische en operationele sturing komen wij tot de volgende tussenconclusies, die wij opnieuw als praktijkbevindingen weergeven.

Praktijkbevinding 2a: Er is een functionerend stelsel van stuurploegen die strategische beleidsbeslissingen nemen.

Praktijkbevinding 2ba: De strategische beleidsbeslissingen worden traag omgezet in uit te voeren beleid. Van strategische sturing van de werkvloer is nog weinig sprake.

Praktijkbevinding 2bb: Er is een groot verschil tussen de (gedocumenteerde) werkelijkheid en de praktijk van de werkvloer, hetgeen ertoe leidt dat strategische besluitvorming beperkt wordt geaccepteerd door de medewerkers van de werkvloer.

Praktijkbevinding 2c: Er is geen sprake van een eenduidig strategisch beleid. Het strategische beleid is versnipperd en dat maakt het uiteindelijk ineffectief.

Praktijkbevinding 2d: De CIE is haar autonome positie met betrekking tot de eigen prioriteitenstelling kwijtgeraakt en is in toenemende mate ondergeschikt geraakt aan het algemene strategische beleid.

Praktijkbevinding 2e: De CIE en de RIO worden in belangrijke mate geregeerd door de waan van de dag. De leidinggevenden reageren op gebeurtenissen, maar nemen nauwelijks proactieve, lange-termijn-beslissingen. Daarnaast kunnen veel leidinggevenden het operationele werk moeilijk loslaten, hetgeen ten koste gaat van de lange termijn sturing.

Praktijkbevinding 2f: De operationele en tactische sturing door middel van het systeem van briefing en debriefing vindt deels plaats en deze praktijk neemt toe. Met name het debriefen gebeurt in de praktijk veelvuldig. Omdat er echter nauwelijks wordt gebriefd, is er van een daadwerkelijke operationele en tactische sturing zoals bedoeld binnen IGP nauwelijks sprake.

Praktijkbevinding 2g: Bij de CIE en de RIO is er sprake van een *street-level bureaucracy*, waarbij de medewerkers op de werkvloer een grote discretionaire ruimte hebben. Dit maakt de medewerkers erg moeilijk te sturen.

Praktijkbevinding 2h: Binnen de CIE en de RIO is sprake van een tweedeling tussen een *street-cop culture* en een *management-cop culture*. Dit belemmert in bepaalde gevallen de sturing in de praktijk.

Concluderend

Op basis van de bovenstaande praktijkbevindingen concluderen wij dat het sturen van de politieorganisatie één van de grote uitdagingen voor de succesvolle implementatie van IGP blijft. Op het moment van het afronden van het veldwerkonderzoek (tot aan maart 2011) is er in ieder geval nauwelijks sprake van sturing op operationeel, tactisch en strategisch niveau. We hebben voorts geconstateerd dat analyseproducten nog steeds weinig worden gebruikt bij de sturing van de CIE en de recherche in bredere zin. De achterliggende reden hiervoor ligt in de gebrekkige acceptatie van criminaliteitsanalyse binnen de politie. Alhoewel de discipline van criminaliteitsanalyse al sinds de jaren ‘70 en ‘80 van de vorige eeuw door politieorganisaties is gebruikt (zie Fijnaut en Moerland 2000: 23 e.v.), is de acceptatie ervan anno 2012 klaarblijkelijk nog steeds geen automatisme (zie ook: Cope 2004). We zullen in sectie 7.5 verder stilstaan bij de analyse in de praktijk.

7.3 Verzamelen van informatie in de praktijk

In deze sectie behandelen wij de wijze waarop de verzameling van informatie in de praktijk vorm krijgt. De organisatorische eenheid CIE is primair belast met het

verzamelen van informatie door middel van het runnen van informanten. In deze sectie zullen wij dan ook met name de CIE behandelen. Met betrekking tot het verzamelen van informatie gelden binnen IGP twee belangrijke uitgangspunten. Allereerst dient IGP de CIE (en de RIO's) proactiever te maken. Zij dienen te anticiperen op bepaalde ontwikkelingen op het gebied van criminaliteit. De proactivering van de informatieverzameling is het onderwerp van subsectie 7.3.1. Naast een proactieve informatieverzameling vereist IGP ook dat de informatieverzameling gericht plaatsvindt. Dit is het tweede uitgangspunt en wordt in subsectie 7.3.2 behandeld.

7.3.1 Proactieve informatieverzameling

In zekere zin is een CIE altijd al proactief geweest. De CIE bepaalt immers zelf welke informanten worden aangelopen en doet dit op eigen initiatief. Binnen IGP wordt echter meer verstaan onder proactiviteit. IGP houdt in dat de CIE probeert om vroegtijdig trends en ontwikkelingen te onderkennen. De CIE moet weten wat er binnen 'het milieu' speelt en moet kunnen duiden welke criminaliteitsproblemen nog zullen gaan spelen. Dit wordt ook wel het benoemen van de blinde vlekken genoemd. Wij horen tijdens het veldwerk vaak van CIE-ers dat de CIE 'meer aan de voorkant moet zitten' (zie citaat hieronder; zie ook subsectie 7.1.3). De CIE staat echter pas aan het begin van deze ontwikkeling. Het proactiveren van de CIE blijkt in de praktijk een zeer moeizaam proces te zijn. Zoals reeds eerder gezegd, wordt de CIE voor het grootste deel geregeerd door de waan van de dag (zie sectie 7.2). Een runner verwoordt dit als volgt.

"*Ik denk dat we wat meer op het randje zijn beland waarbij we de vraag moeten gaan beantwoorden van waar willen we als dienst naartoe? Willen we echt als een inlichtingendienst gaan werken en stappen we af van het klakkeloos bedienen van tactiek en gaan wij ons meer richten op wat we zien in het milieu, wat zijn de trends en de ontwikkelingen.*" Runner CIE (D), maart 2011.

In deze subsectie bezien wij waarom de CIE moeite heeft om proactiviteit in de zin van IGP te bereiken. Wij behandelen daartoe allereerst (A) de afhankelijkheid van de CIE van de informanten. Daarna gaan wij in op (B) de afhankelijkheid van de CIE van tactische opsporingssuccessen, (C) de rol van moderne technologieën binnen de CIE en (D) veranderende aandachtsgebieden.

A: De afhankelijkheid van informanten

Eén van de problemen van de CIE is dat zij afhankelijk is van informatie van informanten. Zij heeft feitelijk bijna geen andere mogelijkheden om informatie te verzamelen. Informanten-informatie is echter zachte informatie, en in veel gevallen is de betrouwbaarheid ervan moeilijk in te schatten. Een hoofd CIE verwoordt dit als volgt.

"*Wij hebben een groot probleem met het inschatten van de betrouwbaarheid van onze informanten. De CIE runt altijd in een wereld van onbetrouwbare figuren: daarom ben ik altijd terughoudend met een informant op een 4*4 (*thans 4*3 genoemd, opmerking auteur*) aan te merken als betrouwbaar. Ze komen met de wildste verhalen en hebben allemaal een eigen agenda. Je hebt dus te maken met echt zachte*

informatie waarvan je niet weet wat je er precies mee kunt." Interview hoofd CIE (A), mei 2007.

Volgens sommige respondenten valt de informatiepositie van de CIE doorgaans tegen. Het duurt erg lang om een informatiepositie te verkrijgen, en volgens enkele runners wordt er te weinig stelselmatig geïnvesteerd in het vinden van nieuwe informanten. Een aanzienlijk deel van het informantenbestand bestaat volgens deze respondenten ook uit 'oude bronnen' (informanten die al een lange tijd worden gerund).

Of er nieuwe informanten worden benaderd hangt vaak af van een runners-koppel zelf. Hier wordt weinig op gestuurd (de sturing van de informatieverzameling is het onderwerp van de volgende sectie). Overigens betekent de eis van een gerichte sturing niet dat de CIE alleen maar werkt op bepaalde van tevoren vastgestelde onderwerpen. Het wordt van de CIE ook verwacht dat zij 'breed runt', hetgeen betekent dat zij oog heeft voor mogelijke nieuwe onderwerpen waar de politie tot dan toe nog geen aandacht voor heeft gehad. In dit opzicht is het aan de CIE om als het ware de afzetmarkt voor haar informatie- en inlichtingenproducten te vormen: zij moet als eerste bepaalde trends en ontwikkelingen signaleren. Een proactieve CIE zal dan ook in staat moeten zijn om de doelstellingen van de komende periode mede helpen vorm te geven.

B: De afhankelijkheid van tactische opsporingssuccessen

Uit ons veldwerk blijkt dat de CIE sterk afhankelijk is van de tactische opsporingsteams: die vormen als het ware de 'afzetmarkt' voor CIE-informatie. De waarde van CIE-informatie wordt doorgaans bepaald aan de hand van de mate waarin de informatie door een concreet tactisch opsporingsteam kan worden gebruikt. Het gaat daarbij om processen-verbaal die de CIE-en aan tactische opsporingsteams verstrekken. Het beeld bestaat dat niemand zit te wachten op CIE-informatie die niet direct bijdraagt aan operationele successen in tactische onderzoeken. CIE-en richten zich met name op de bestaande afzetmarkt voor processen-verbaal, en dit is ook waar de effectiviteit en efficiency van de CIE op worden beoordeeld. In het verlengde hiervan ligt een andere reden om met name informatie in te winnen die direct in een opsporingsonderzoek kan worden gebruikt: de beloningsstructuur voor informanten.

De beloning voor informanten wordt ook wel 'tipgeld' genoemd, en de basis voor de tipgelden is de Circulaire bijzondere opsporingsgelden.[253] Tipgeld wordt als hoofdregel uitgekeerd als de door de informant verstrekte inlichtingen (mede) hebben geleid tot het ophelderen van een strafbaar feit, aldus artikel 1 sub c onder i en ii Circulaire bijzondere opsporingsgelden. Dit is een soort '*no cure, no pay*' uitgangspunt (zie ook Van der Bel et al. 2009: 106-107). Tipgeld wordt dus uitgekeerd in geval van een tactisch succes. Wij maken een onderscheid in twee categorieën van tactische successen. De eerste categorie zijn de directe tactische successen, zoals een veroordeling in eerste aanleg, een inbeslagname van contant geld of andere waardevolle goederen en de aanhouding van een verdachte en een daaropvolgende positieve vervolgingsbeslissing. De tweede categorie zijn de indirecte tactische successen. Zo kan een informant tipgeld krijgen indien zijn informatie bijdraagt tot het in kaart brengen van een crimineel samenwerkingsverband (CSV), mits dit leidt tot de start van een opsporingsonderzoek (zie ook artikel 1 sub c onder

[253] Circulaire Bijzondere Opsporingsgelden, Stcrt. 2012, 5545.

viii). Een ander voorbeeld van een indirect tactisch succes is dat een informant wordt beloond indien hij goede informatie heeft verstrekt, maar de informatie niet leidt tot een opsporingsonderzoek vanwege prioriteitsredenen (dit is een soort *escape*-mogelijkheid om in bepaalde gevallen toch nog over te kunnen gaan tot het betalen van tipgelden indien zeer goede informatie zoals gezegd niet leidt tot de start van een opsporingsonderzoek, zie artikel 1 sub c onder vi Circulaire bijzondere opsporingsgelden).

Voor zowel de directe als de indirecte tactische successen geldt dat het beloningssysteem helemaal is afgestemd op de tactische opsporing. In de praktijk leiden de directe tactische successen tot een snellere en doorgaans hogere beloning dan de indirecte successen. Maar wat te doen met de informant die waardevolle inzichten verschaft in de sociale verhoudingen en ontwikkelingen in het criminele milieu? Deze informatie leidt zelden tot directe tactische opsporingssuccessen en lang niet altijd tot indirecte opsporingssuccessen.

Wij constateerden tijdens ons veldwerk dat CIE-runners de beloningen voor de informanten als een belangrijk bindmiddel beschouwen en dat zij daarom de nadruk leggen op het verzamelen van informatie die leidt tot de directe successen (en in mindere mate tot indirecte successen). De nadruk ligt daarmee op het verzamelen van informatie die een bijdrage kan leveren in lopende opsporingsonderzoeken of informatie waarvan van tevoren de kans op tactische successen het grootst lijkt. Dit betreft de bekende en geëigende onderwerpen, zoals de handel in verdovende middelen en onderzoeken naar bekende topcriminelen. Andere onderwerpen die minder voor de hand liggen worden minder snel door de CIE opgepakt.

Binnen IGP lijken de voornoemde directe en indirecte tactische successen in toenemende mate ondergeschikt aan het geven van voorwaarschuwingen en een brede, integrale aanpak van criminaliteitsproblemen. In de praktijk levert dit veel minder tipgeld op dan de directe en indirecte successen. Voor de runners betekent dit dat er geen aansporing is om informanten te verkrijgen die een breed inzicht kunnen verschaffen. Voor IGP is de hiervoor geschetste situatie onwenselijk. Het leidt er namelijk toe dat de CIE met name informatie inwint op onderwerpen waarin zij directe en indirecte tactische successen kan behalen. Dit betekent dat de aandachtsgebieden waarop een CIE zich richt primair worden vastgesteld door de behoeften en belangen van de overige tactische rechercheafdelingen. De CIE blijft op deze manier een reactief organisatieonderdeel.

C: Nieuwe technologieën binnen de CIE

Nieuwe technieken zoals *datamining* en informatiefiltering moeten het mogelijk maken om gericht informatie uit grote hoeveelheden data te destilleren. In de praktijk hebben wij verschillende systemen gezien die op één of andere manier aan *datamining* doen. Overigens worden deze technieken doorgaans niet binnen de CIE toegepast, maar binnen de RIO. In vrijwel alle gevallen worden de systemen getest in situaties die voor ons onderzoek niet toegankelijk waren. In de door ons onderzochte korpsen is *datamining* nog niet toegepast in een operationele omgeving.

Een ander onderwerp dat voor het verzamelen van informatie van belang kan zijn, is *profiling*. Evenals bij *datamining* wordt *profiling* nog met name in test-omgevingen uitgeprobeerd. Wij zijn het nog niet tegengekomen in een operationele setting. Met betrekking tot deze twee nieuwe technologieën constateren wij dat ze binnen de CIE niet worden toegepast. De CIE is een vrij conservatieve organisatie die moderne ontwikkelingen en technologieën niet snel zal gebruiken (zie ook Kop et al.

2007: 62). Wij kunnen deze bewering op basis van ons onderzoek onderschrijven: de CIE werkt tijdens ons onderzoek grotendeels op dezelfde wijze als bij de oprichting van de eerste CID-en (zij het dat er vandaag de dag veel meer juridische kaders zijn waaraan de CIE zich dient te houden).

D: Veranderende aandachtsgebieden

Een belangrijke verandering binnen de CIE-en op het gebied van proactieve informatieverzameling is dat de georganiseerde criminaliteit complexer is geworden en dat de CIE zich hieraan moet aanpassen. Dit heeft te maken met de (onder andere door nieuwe technologieën) complexer wordende samenleving, maar ook met een steeds duidelijkere verwevenheid tussen de 'onder- en bovenwereld' (zie Kop et al. 2007: 21). De CIE verzamelt inlichtingen echter met name in het traditionele criminele milieu. IGP stelt bepaalde eisen aan de CIE en de CIE zal zich daarom dienen aan te passen. De CIE is zoals gezegd echter niet snel geneigd om innovaties toe te passen binnen het criminele inlichtingen proces. In tegenstelling tot een aantal jaren geleden zal de CIE zich bijvoorbeeld meer moeten gaan richten op het runnen in de zogenoemde 'bovenwereld' (Kop et al. 2007). Aan een runner in de bovenwereld dienen andere eisen te worden gesteld dan aan de klassieke runner (Kop et al. 2007: 91). Dit blijkt ook uit onze gesprekken met respondenten.

"*(…) wat ik nu ga zeggen is helemaal listig en lastig, als je kijkt naar een CIE-apparaat of orgaan, dan moet je daar een afspiegeling hebben van de maatschappij. Daar moet je jonge gasten tussen hebben zitten, daar moet je vrouwen tussen zetten, van alles wat, en niet het klassieke model dat je mannen op de gymschoenen achterna gaat. Je moet mensen hebben die een waardig gesprekspartner kunnen zijn, voor dat gebied waar je op gaat acteren.* " Interview teamleider tactiek (B), mei 2009.

Ook voor het runnen op terrorisme geldt dat hiervoor andere eisen dienen te worden gesteld dan aan het runnen op de klassieke onderwerpen. Terrorisme (en links of rechts extremisme) zijn hele andere onderwerpen dan de traditionele georganiseerde criminaliteit en vereisen ook een ander profiel van runner. Een zij-instromer benoemt het als volgt.

"*Het is niet meer zoals vroeger. Je zit in een wereld die internationaal en digitaal is. Het wordt zo complex. Een onderwerp als terrorisme is niet de standaard drugszaak. Daar zitten zoveel andere elementen in. En hetzelfde geldt voor internationale misdrijven, ook dat is een heel complex aandachtsgebied. En high tech crime bijvoorbeeld, daar merk je ook dat mensen in het MT en rechercheurs veel minder mee hebben. Die draaien helemaal niet graag zo'n zaak. Ook een terreurzaak, dat duurt waarschijnlijk weer te lang, je ziet vaak ook weinig, en op een gegeven moment denken die rechercheurs in een team dat ze voor niks aan het werk zijn en dat het niet opschiet. Ze houden van actie en ze willen voortgang zien. Ze hebben gewoon geen geduld. Ze zijn gewoon van dag tot dag aan het werk met planning enzo...*" Interview recherchekundige RIO (A), mei 2010.

Zowel voor runnen in de bovenwereld als voor runnen op terrorisme geldt dat de runners over een zekere expertise en specifieke kwaliteiten dienen te beschikken. Doorgaans wordt van runners echter verwacht dat ze overal iets van af weten en dat ze op alle onderwerpen kunnen runnen. Van een concreet beleid om de juiste mensen

aan te nemen die op deze onderwerpen een verregaande expertise hebben, is nog geen sprake. Langzaamaan ontstaat er binnen verschillende regio's wel het besef dat onderwerpen als terrorisme, *high-tech crime* of witwassen een specifiek profiel van runners nodig hebben. Men probeert opleidingen en cursussen te ontwikkelen die aan deze behoefte kunnen voldoen, maar dit is nog geen gestandaardiseerde praktijk. Binnen de CIE-en verkrijgen sommige koppels een bepaalde expertise-status op de genoemde onderwerpen, maar het gebeurt doorgaans op initiatief van de runners zelf. En sommige onderwerpen, zoals terrorisme, blijken in de praktijk een stuk minder aantrekkelijk dan men zich had voorgesteld (zie subsectie 8.2.5). Als de CIE runners met een bijzondere achtergrond, expertise of opleiding wil binnenhalen, dan zal zij ook bereid moeten zijn om daarvoor te betalen.

Al met al stellen wij vast dat de informatieverzameling door de CIE nog niet echt proactief te noemen is. De vraag die nu rijst, is in hoeverre de informatieverzameling gericht is. Dit is het onderwerp van de volgende subsectie.

7.3.2 Gerichte informatieverzameling

Voor de CIE betekent een proactieve werkwijze ook dat zij op basis van analyseproducten gericht nieuwe informanten zal moeten zoeken en bestaande informanten bevragen en proberen een antwoord te krijgen op de vragen die op dat moment actueel zijn en bijdragen aan bepaalde inzichten en oplossingen. Het kost de CIE echter veel tijd om op een bepaald onderwerp een informatiepositie te verkrijgen. Dit heeft te maken met het feit dat het opbouwen van een relatie met potentiële informanten een lange tijd in beslag neemt. De meeste informanten zullen niet tijdens het eerste gesprek alles vertellen wat ze weten, maar verschaffen doorgaans pas relevante inlichtingen wanneer er een vertrouwensrelatie met de runners is opgebouwd (als ze dit ooit al doen). Een CIE is dus gebaat bij duidelijke doelstellingen op basis waarvan zij een informatiepositie dient te verkrijgen: de verzamelde inlichtingen moeten wel opwegen tegen de investering in tijd en capaciteit. Daarnaast is het voor een CIE belangrijk om gericht te werk te gaan omdat er veel meer informatie verzameld kan worden dan de CIE of de RIO kan verwerken. Het is voor de CIE al bijna onmogelijk om de inlichtingen afkomstig van informanten tijdig te verwerken, laat staan wanneer daar bijvoorbeeld nog extra informatie uit open-bronnen bij komt. Het gericht sturen van de CIE betekent dat er een keuze wordt gemaakt in de onderwerpen waarop de CIE dient te werken. De door de landelijke stuurploeg en de regionale stuurploeg vastgestelde prioriteiten zijn een goede eerste indicatie voor deze keuze. Deze prioriteiten zijn met name strategisch van aard: ze geven aan waar de algemene prioriteiten van de politie liggen. Dergelijke algemene prioriteiten bieden echter geen goede aanknopingspunten voor de gerichte operationele en tactische informatie-inwinning door de CIE. Een CIE zal specifiek moeten weten wat er wordt verwacht. Gaat het bij mensenhandel bijvoorbeeld om de aanpak van illegale prostitutie, of illegale zwartwerkers in de land- en tuinbouwsector? Beide vereisen een andere benadering door de CIE (andere soort informanten, andere mogelijke interventies, andere partners die bij de bestrijding kunnen worden betrokken et cetera).

In de praktijk constateren wij dat er nog weinig concrete invulling is gegeven aan de onderwerpen die zijn geprioriteerd, hetgeen een gerichte sturing op informatie door de CIE bemoeilijkt. Wij hebben in ieder geval weinig uitgewerkte strategische plannen gezien waarin bijvoorbeeld duidelijk wordt (1) wat het doel is van de gekozen aanpak, (2) wanneer de aanpak succesvol wordt beoordeeld, (3) welk

tijdspad er is gekozen en (4) wie welke verantwoordelijkheden krijgt. Voor een CIE blijkt het dan ook bijzonder lastig om een benadering te kiezen. De onderwerpen zullen nader moeten worden uitgewerkt voordat ze de basis bieden voor een gerichte aansturing van de CIE. Het is aan de CIE-en van de politiekorpsen zelf om de onderwerpen verder uit te werken, en hieraan wordt op verschillende wijzen invulling gegeven.

Tijdens ons veldwerk blijkt dat de meeste CIE-en nauwelijks structureel met de regionale of landelijk vastgestelde prioriteiten werken. Eén CIE is hiermee echter wel erg ver. Er wordt daar gewerkt met bepaalde beleidsmatige programma's op specifieke onderwerpen (zie subsectie 7.2.1). Het is de bedoeling dat de CIE informanten werft die met name over de in de programma's geformuleerde doelstellingen informatie verstrekken. Dit is althans op papier het geval. In de praktijk blijkt dat het nog niet helemaal loopt zoals het moet. Deze gedachte wordt ondersteund door een geïnterviewde teamleider.

"*We hebben een aantal programma's (…). Die targets zijn genoemd. Als die targets zijn benoemd, dan verwacht ik van de CIE dat zij zorgen dat zij informatieposities creëren rondom de targets. Dat ze dat niet volgende week hebben, dat spreekt voor zich. Maar na verloop van tijd zou dat wel moeten, en zo zou het bij elk programma moeten (...). Mijn vraag is dan: heb ik de indruk dat ze op de aandachtsgebieden een redelijke positie hebben? Daarop ben ik geneigd te zeggen dat het wel beter zou kunnen, moeten en mogen."* Interview teamleider tactiek (B), mei 2009.

In deze gevallen zijn er wel keuzes gemaakt, maar wij constateren dat ze door de werkvloer veelvuldig worden bekritiseerd. Wanneer er wordt gekozen om de aandacht slechts te richten op de export van een specifieke soort verdovende middelen naar bijvoorbeeld België, dan vragen de rechercheurs en analisten zich af waarom men ook niet naar de import kijkt. Immers, als de import wordt bemoeilijkt, dan zou dat ook de export raken. Zo kan iedere beslissing rekenen op kritiek. De beslissingen die worden genomen, worden zelden toegelicht en zijn daarom voor de medewerkers op de werkvloer soms onbegrijpelijk. Deze medewerkers worden nauwelijks actief betrokken bij het proces van de besluitvorming. Dit is ook niet verwonderlijk: je kunt nu eenmaal niet iedereen betrekken bij besluitvorming. Zoals echter in subsectie 7.2.2 al is beschreven, is een dergelijke *top down* sturing van de politieorganisatie vanwege de *street-level bureaucracy* en de scheiding tussen de cultuur van de uitvoerenden en de cultuur van de leidinggevenden erg moeilijk: dit kan rekenen op kritiek en, in bepaalde gevallen, verzet.

Een bijkomende moeilijkheid van de hierboven genoemde gerichte, programmatische sturing is dat de programma's en de informatiebehoeften in toenemende mate door de RIO worden vastgesteld, en niet door de CIE zelf. Omdat de RIO (nog) geen autorisatie heeft voor de 00, 200 en 300 informatie van de CIE, zijn de door hen vastgestelde programma's en inwinplannen niet volledig. Er vindt dus sturing plaats met een deel van de informatie. De CIE heeft wel het complete informatie-overzicht en de medewerkers van de CIE geven aan dat ze in bepaalde gevallen zelfstandig een inwinplan opstellen. Een centrale sturing van de CIE wordt op deze manier aanzienlijk bemoeilijkt.

7.3.3 Tussenconclusies

Met betrekking tot het verzamelen van informatie kwamen wij tot de volgende tussenconclusies die ook hier praktijkbevindingen worden genoemd.

Praktijkbevinding 3a: De CIE werkt in hoge mate nog steeds reactief. Een proactieve werkwijze zoals vereist binnen IGP wordt niet bereikt omdat de CIE (1) afhankelijk is van informanten, (2) afhankelijk is van tactische opsporingsteams en (3) nauwelijks gebruik maakt van technologische innovaties.

Praktijkbevinding 3b: Er wordt weinig met informatie gestuurd. De CIE maakt weinig structureel gebruik van informatieproducten bij het sturen van het inwinnen van informatie.

Praktijkbevinding3c: De CIE maakt nauwelijks gebruik van objectief vastgestelde prioriteiten, maar bepaalt grotendeels zelfstandig op welke onderwerpen informatie wordt verzameld.

Concluderend

Op basis van de hierboven geformuleerde praktijkbevindingen komen wij tot de volgende conclusie met betrekking tot het verzamelen van informatie. IGP gaat uit van een proactieve informatieverzameling waarbij de CIE zelfstandig op zoek gaat naar relevante criminele inlichtingen zonder zich teveel te laten leiden door de waan van de dag. De CIE werkt met betrekking tot het verzamelen van informanteninformatie echter grotendeels nog steeds op dezelfde manier als waarop ze voor IGP werkte. In de praktijk is er dus erg weinig veranderd: de CIE is nog steeds voor een aanzienlijk deel primair een reactief organisatieonderdeel.

7.4 Verwerken van informatie in de praktijk

Nadat informatie is verzameld, wordt het opgeslagen in de politiële systemen. De fase van verwerking ziet dus op (1) de informatiehuishouding en (2) de bijbehorende ICT van de politie. Beide zaken hebben te maken met de kwaliteit van informatie en zijn daarom van groot belang voor IGP. In dit opzicht geldt de ICT-stelregel *rubbish in, rubbish out:* als de kwaliteit van de invoering en verwerking van de verzamelde informatie slecht is, dan zullen de informatieproducten die daarop worden gebaseerd eveneens van een slechte kwaliteit zijn. Bij het verwerken van informatie door de CIE moet er een onderscheid worden gemaakt tussen twee soorten informatie: (1) de informanten-informatie (subsectie 7.4.1) en (2) de rest- en zijtak-informatie (subsectie 7.4.2).

7.4.1 Informanten-informatie

Voor de CIE is informanten-informatie de belangrijkste vorm van informatie. Informanten-informatie (in inlichtingenjargon ook wel *human intelligence* genoemd, oftewel HUMINT) is echter een bijzondere vorm van informatie. Het gaat vaak om subjectieve verhalen van gebeurtenissen uit de tweede of derde hand. Het wordt daarom ook wel ‘zachte informatie’ genoemd. In deze subsectie behandelen wij de volgende drie elementen van informanten-informatie: (A) de mate waarin

informanten-informatie als zachte informatie kan worden aangemerkt, oftewel de beoordeling van de betrouwbaarheid van de informant en diens informatie, (B) hoeveel informanten-informatie daadwerkelijk de systemen bereikt en (C) de informatiesystemen waarmee de CIE/RIO werkt.

A: Beoordeling betrouwbaarheid informant en informatie

De controle van de betrouwbaarheid van de informant en de informatie is een essentieel onderdeel van het CIE-proces en van groot belang voor IGP. Immers, de kwaliteit van intelligenceproducten is afhankelijk van de kwaliteit van de gebruikte informatie. Er moet echter een onderscheid worden gemaakt tussen de betrouwbaarheid van de informant en de betrouwbaarheid van de informatie. Een informant kan betrouwbaar zijn, maar onbetrouwbare informatie verstrekken, bijvoorbeeld omdat hij iets verkeerd heeft verstaan of omdat iemand anders hem heeft voorgelogen. En een doorgaans onbetrouwbare informant kan betrouwbare informatie verstrekken, bijvoorbeeld omdat zijn persoonlijke belangen hem ertoe brengen 'de waarheid' te vertellen (voor zover mogelijk). Wij werden tijdens ons onderzoek door diverse respondenten gewezen op dit relevante onderscheid. Eén respondent verwoordt het als volgt.

"*Ik vind iets pas echt betrouwbaar als ik een bevestiging uit een heel andere hoek heb, dan zou ik zeggen de conclusie is, gelet op de mij bekende persoon, en de aard van de informatieverzameling, ik vind dit betrouwbaar. En dan nog geldt: garantie tot aan de deur. Want CIE-info kan bij nader onderzoek gewoon niet blijken te kloppen. Het gaat dan om een informant die iets gehoord heeft in een café en die dat netjes één op één vertelt. Of het waar is, is maar de vraag.*" Interview hoofd CIE (B), februari 2009.

Verschillende respondenten geven aan dat de betrouwbaarheid van de informant en diens informatie eigenlijk niet te beoordelen is omdat het inwinproces in het algemeen is versnipperd. Er is slechts een beperkt aantal controlemethoden waarover de CIE zelfstandig beschikt. Wij noemen er drie. Allereerst kan de CIE informanten en informatie controleren door meerdere informanten te zoeken die in een bepaalde relatie tot elkaar of tot bepaalde informatie staan. Zo kan er worden gekeken of de door de informant verstrekte informatie overeenkomt met de informatie die andere informanten hebben verstrekt. Dit wordt in de praktijk niet structureel toegepast. De tweede controlemogelijkheid is dat de CIE de betrouwbaarheid van de informanten en informatie beoordeelt door open bronnen te raadplegen. Net als de eerste methode wordt deze methode in de praktijk echter niet structureel toegepast, omdat open-bronnen-informatie (zoals het internet) volgens runners weinig aanknopingspunten bieden voor een dergelijke controle. Met name de klassieke informanten-informatie met betrekking tot traditionele criminaliteit blijkt moeilijk te controleren aan de hand van open bronnen. CIE-en zijn echter niet snel geneigd om te experimenteren met mogelijke (technologische) oplossingen waarbij open bronnen worden betrokken (zie subsectie 7.3.1). De derde mogelijkheid die wij noemen is het spiegelen van informanten-informatie aan de overige informatie die binnen de politie aanwezig is, zoals informatie uit tactische opsporingsonderzoeken. Soms blijkt uit tactische informatie dat bepaalde informanten-informatie al dan niet betrouwbaar is, maar dit is niet zelden min of meer toevallig. Methode twee en drie vinden doorgaans tijdens het veredelingsproces plaats (zie hiervoor subsectie 4.5.2).

Voor alle drie genoemde controlemethoden geldt dat ze zeer bewerkelijk zijn en erg veel tijd en moeite kosten. Daarnaast heeft de CIE slechts in kleine mate de regie over deze controlemethoden: voor het runnen van informanten gelden erg strenge regels (zie sectie 4.4), de informatie uit open bronnen wordt door anderen geselecteerd en gepubliceerd en informatie uit opsporingsonderzoeken wordt door tactische opsporingsteams verzameld en vastgelegd. De invloed van de CIE over al deze methoden is zeer klein en de inspanning om de informant en diens informatie te controleren lijkt verhoudingsgewijs te groot voor wat het oplevert. Dit leidt ertoe dat de CIE van de genoemde controlemethoden in de praktijk niet structureel gebruik maakt. De CIE zet ook geen opsporingsbevoegdheden uit de Wet BOB in ten behoeve van de controle van de informant of diens informatie.

De vraag die nu rijst, is hoe de CIE de betrouwbaarheid van informanten beoordeelt. Vaak wordt een informant als betrouwbaar beoordeeld indien hij in het verleden betrouwbaar is gebleken. Een runner stelt hierover het volgende.

"*Men kijkt vaak naar hoe lang een informant al in dienst van ons is. Er wordt gekeken naar hoe vaak de informant een verhaal heeft neergelegd wat tactisch is opgevolgd en juist is gebleken. Dat laatste is denk ik het voornaamste. Als een informant vaak een verhaal vertelt wat na een tactisch vervolg juist is gebleken dan wordt de status een A of een B gegeven (...). Eigenlijk kunnen we niet goed beoordelen of informatie betrouwbaar is.*" Interview runner CIE (D), maart 2011.

In andere gevallen spreekt een informant bijvoorbeeld over een aantal bekende criminelen en levert de informatie in eerste opzicht een beeld op van deze subjecten. Niet zelden betreft het 'spannende verhalen'. Het veronderstelde niveau van de criminelen waarover wordt gesproken en de 'zwaarte' van het verhaal leiden ertoe dat de informatie sneller als betrouwbaar wordt aangemerkt. Dit is een vorm van de cognitieve vooroordelen (*cognitive biases)* die Heuer (1999: 116-119) onderscheidt: "*information that is vivid, concrete, and personal has a greater impact on our thinking than pallid, abstract information that may actually have substantially greater value as evidence.*" Het feit dat runners het verhaal persoonlijk van een bron vernemen, maakt dat ze meer gewicht aan dat verhaal toekennen dan aan andere, afwijkende informatie. Deze cognitieve vooroordelen spelen overigens ook een rol bij de hiervoor genoemde controlemogelijkheden: informatie afkomstig van open bronnen, politiesystemen of andere informanten wordt vanwege het cognitieve vooroordeel snel verworpen.

Wanneer toch gebruik wordt gemaakt van de controlemethoden ten behoeve van de veredeling van ingewonnen inlichtingen, is het een risico dat men zoekt naar bevestigende informatie in plaats van ontkrachtende informatie. Dit wordt ook wel *confirmation bias* genoemd, een bekend fenomeen binnen de inlichtingen- en veiligheidsdiensten (zie: Johnston 2005: 21-25; zie voor tunnelvisie bij de politie: Posthumus 2005: 170 e.v.). Hierin schuilt volgens enkele respondenten een gevaar. Omdat er beperkte analysecapaciteit bij de CIE is, zijn het vaak de runners zelf die deze veredeling doen. Sommige runners beschikken volgens respondenten niet over de kwaliteiten of mogelijkheden om bijvoorbeeld te waken voor tunnelvisie. Zij zijn (zoals een ieder in hun plaats) onderhevig aan de hiervoor beschreven cognitieve vooroordelen en *confirmation bias*. In veel gevallen laat de veredeling dan ook te wensen over. Omdat de runners de veredeling meestal als een administratieve last ervaren (en dus wellicht niet naar behoren uitvoeren), wordt dit door sommige grotere CIE-en die beschikken over medewerkers ten behoeve van de administratieve

ondersteuning overgelaten aan deze medewerkers. Het is voor deze medewerkers echter niet te doen om alle informatie te veredelen, en zij zijn daartoe zelden opgeleid. Zij kijken naar een beperkte hoeveelheid (openbare) bronnen, beoordelen of de door de informant genoemde namen kloppen en vullen de gegevens indien nodig aan met andere informatie. Een verregaande inhoudelijke controle van de informatie is er niet bij. Dit zou in principe door analisten gedaan moeten worden. Zoals we later nog zullen betogen, heeft de CIE de analysetaak in het verleden echter onvoldoende uitgevoerd en mist zij daarom analysecapaciteit (zie sectie 7.5).

Wat volgens respondenten ook vaak voorkwam, is dat wanneer elementen van een verhaal blijken te kloppen, de rest van het verhaal ook voor waar wordt gezien. Als een informant bijvoorbeeld vertelt dat Thijs Vis (a) in Utrecht woont, (b) in een Mercedes rijdt, (c) rechten heeft gestudeerd en (d) een vuurwapen heeft, dan zal een eenvoudige zoekslag in open bronnen aantonen dat a, b en c juist zijn. Dit maakte soms dat d dan ook als waar wordt beoordeeld. Het gaat te ver om deze cognitieve psychologische processen hier verder te behandelen (zie hiervoor: Heuer 1999; Johnston 2005). Voor ons volstaat het te constateren dat een dergelijke 'veredeling' (die naam mag het eigenlijk niet dragen) tot onjuiste conclusies en vervuilde informatiesystemen zal leiden. Ook hier geldt de regel: *rubbish in, rubbish out*. Wij hebben geen verder onderzoek gedaan naar de exacte aard en omvang van deze problematiek en zullen hierover dan ook geen uitspraken doen. Wij volstaan met de vaststelling dat deze problematiek voorkomt bij de CIE, waarmee wij niet zeggen dat hier in alle gevallen bij alle CIE-en sprake van is.

De beperkte controlemogelijkheden leiden ertoe dat de betrouwbaarheid van CIE-informatie doorgaans als 'niet te beoordelen' wordt aangemerkt. Het is een CIE echter grotendeels niet aan te rekenen dat veel van haar informatie niet te beoordelen blijkt: in tegenstelling tot de AIVD, die diverse inlichtingenmiddelen kan inzetten om informanten en agenten (en hun informatie) te controleren, beschikt de CIE voor een goede betrouwbaarheidstoets niet over dergelijke middelen. Dat gezegd hebbende, constateren wij echter ook dat de CIE-en weinig gebruik maken van de middelen die zij wel tot hun beschikking hebben.

Een oplossing voor het probleem van de beoordeling van betrouwbaarheid van de informant en de informatie zou kunnen zijn om een deel van de veredeling over te laten aan de medewerkers van de RIO. Zij beschikken immers over de analysecapaciteit en de tijd om ook de tactische informatie te betrekken bij het beoordelen van informatie. Verschillende respondenten wijzen ons echter op het feit dat CIE-informatie door politiemensen die niet bij de CIE werken te vaak al te snel als te 'waardevol' wordt aangemerkt. De gedachtegang is dat omdat de CIE een geheime dienst is, de door haar verzamelde informatie wel juist moet zijn (zie ook: Johnston 2005: 24). Mensen met een CIE-achtergrond zijn doorgaans erg kritisch op CIE-informatie en wezen ons op de beperkingen ervan. De gedachte wordt hieronder als volgt onderstreept.

"*En wat ik nog even wil benadrukken, is waarom CIE'en terughoudend zijn met het uitbreiden van een groep geautoriseerden. De reden is dat dingen een eigen leven gaan leiden. Er zijn twee elementen belangrijk: (A) kun je het in de context plaatsen? (…) En (B) klopt dat wel? (Het) is een verhaal. (…) Het is natuurlijk het tuig van de richel waarmee wij praten, die altijd een eigen belang hebben met het verhaal dat ze vertellen. Ze laten natuurlijk dingetjes weg, vooral waar ze zelf in voorkomen, dikken dingen aan, want dat gaat over Gerrit en daar heb ik wel zo'n teringhekel aan, maak zijn rol even wat belangrijker. Dat zijn elementen die zitten allemaal in de verhalen*

van informanten en daar moet je rekening mee houden. Dat maakt ook dat je goed moet weten wat je zegt. Wat is de aannemelijkheid van het verhaal, in hoeverre zou het waar kunnen zijn en in welke context moet je dat plaatsen. Dat zijn eigenlijk elementen aan dat werk, namelijk dat het verhalen zijn, geen verbalen." Hoofd CIE (B), februari 2009.

Vanwege de geheimhouding en de afscherming is het voor de ontvanger van de informatie vaak moeilijk te toetsen in hoeverre CIE-informatie betrouwbaar of waardevol is. Het lijkt erop dat het feit dat de informatie de status van geheim heeft, leidt tot een snellere acceptatie van deze informatie. In sectie 7.5 zeggen we meer over de gevolgen van geheimhouding. Voor deze sectie volstaan wij met de constatering dat CIE-informatie doorgaans zeer moeilijk te beoordelen bleek, en dat dit in de praktijk dan ook nauwelijks plaatsvond. Voor een concept als IGP, dat draait om informatie, analyses en intelligence, is het wrang om te moeten constateren dat één van de belangrijkste informatiebronnen, te weten de inlichtingen afkomstig van informanten, niet te goed te controleren zijn op betrouwbaarheid.

B: Hoeveel informatie bereikt de systemen?

Het verwerken van informanten-informatie betekent ook dat de inhoud van het gesprek uiteindelijk in de informatiesystemen van de politie belandt. Voor de CIE is dit allereerst BVO-Bruto (Basis Voorziening Opsporing): het afgeschermde informatiesysteem waarin de bruto-gespreksverslagen worden verwerkt. Daarnaast maken de CIE-en ook gebruik van BVO-netto. In dat systeem worden de zwacri-informatierapporten (ZIR, ook wel 4*3 formulieren genoemd) opgeslagen. In de praktijk blijkt er echter tussen de verzamelde en verwerkte informatie een groot verschil te zitten. Wij zijn hiervoor drie redenen tegengekomen: (1) de tijdsdruk die het onmogelijk maakt om alle informatie in de systemen in te voeren, (2) het bruto-netto proces waardoor informatie niet in BVO-netto terechtkomt en (3) het feit dat bepaalde kennis niet geschikt is voor de opname in informatiesystemen.

Met betrekking tot (1) de tijdsdruk constateren wij het volgende. Een medewerker van de CIE (of van een RIO) beschikt eenvoudigweg over te weinig tijd om alle verzamelde informatie te verwerken. Een voorbeeld hiervan betreft het runnen door de CIE. Een gemiddeld gesprek duurt ongeveer een à anderhalf uur (uitschieters zijn gesprekken van vier tot vijf uur).[254] Een deel van het gesprek is sociaal van aard, maar de gesprekken gaan grotendeels over zwacri-gerelateerde onderwerpen. Een gespreksverslag van een runner omvat echter ongeveer twee blaadjes A4-formaat, veel minder dan een gesprek van die tijdsduur normaliter oplevert. Tussen datgene wat besproken is tussen de runner en de informant en de verslaglegging daarvan zit dus een gat. Runners geven aan dat dit inderdaad het geval is, en dat dit komt omdat ze de tijd niet hebben om gesprekken letterlijk uit te werken. Ze vatten het gesprek zo goed mogelijk samen en muteren datgene wat van belang is voor de CIE en voor een eventueel opsporingsonderzoek. Deze samenvattingen van

[254] De complexiteit van het runnersvak wordt wellicht duidelijker als de lezer zich een voorstelling probeert te maken van het runnen. Niet zelden zitten runners en informanten in een kroeg of elders in een openbare ruimte en zij spreken een paar uur met een informant. Tijdens het gesprek kunnen vaak niet al te opzichtig veel aantekeningen worden gemaakt, en in bepaalde gevallen zal de runner bijvoorbeeld steekwoorden in een notitieblok opschrijven. Later zal de runner het gesprek moeten reproduceren en op basis van de steekwoorden zo goed mogelijk een complete beschrijving van het gesprek geven. Zie subsectie 4.3.4 voor een korte behandeling van het runnen in de praktijk.

gesprekken zijn in feite een interpretatie van de runners, waarbij de runners er wel zorg voor dragen dat de interpreatie de letterlijke tekst zo dicht mogelijk benadert. De samenvattingen kunnen zijn gevormd door eerdere ervaringen met dezelfde informant of andere informanten, of door andere ervaringen. Het is in ieder geval geen letterlijke weergave van dat wat tijdens het gesprek is gezegd. Overigens is een letterlijk uitwerking alleen mogelijk in die gevallen waarin gesprekken worden opgenomen, en dit is zeker geen standaard praktijk van de CIE.

Uit ons onderzoek blijkt overigens niet dat de CIE bewust informatie buiten de gespreksverslagen laat die voor de CIE of andere rechercheonderdelen nadelig is, bijvoorbeeld omdat het een verdachte zou vrijpleiten. In tegendeel: deze informatie wordt expliciet opgenomen in de gespreksverslagen, al is het maar omdat de CIE er altijd rekening mee houdt dat de informant dubbelspel speelt en bijvoorbeeld zelf opnames van een gesprek maakt. CIE-ers zijn hiervoor zeer beducht en besteden dan ook veel aandacht aan dit soort informatie. De voor het opsporingsproces nadelige informatie wordt dan ook doorgaans opgenomen in het gespreksverslag. Dit laat onverlet dat er informatie niet in de systemen terecht komt, informatie die vanwege uiteenlopende redenen met name voor analisten relevant kan zijn.

Na de verwerking van de informanten-informatie in BVO-bruto vindt het zogenoemde proces van 'bruto-nettoën' plaats (reden 2). Dit houdt in dat van het bruto-gespreksverslag (de uitwerking van het gehele gesprek door de runner) een samenvatting wordt gemaakt (netto-gespreksverslag of 4x3-tje in het jargon) die door de analisten van een informatieafdeling kan worden gebruikt. Een respondent verwoordt het als volgt.

"*Kijk wat zij* (analisten) *lezen, de 4x3tjes, dat zijn samenvattingen van een groot verhaal. Informanten zijn in gesprek, dat duurt 2 uur, enorm verhaal, blablabla, wij gaan heel kort samenvatten, wat is nu eigenlijk de essentie van wat hij heeft gezegd. Dat kan ook niet anders omdat je anders van die lange lulverhalen zit op te schrijven. Dat doen we ook hoor, we werken het ook helemaal uit, maar voor analisten maken we dat weer behapbaar.*" Interview teamleider RIO (B), februari 2009.

Feitelijk betreft het hier een soort tweede samenvatting (de eerste is al door de runner gemaakt bij het opstellen van het gespreksverslag). Het verschil tussen beide samenvattingen is dat de eerste zoveel mogelijk in de woorden van de informant wordt opgesteld, en de tweede wordt vervormd ten behoeve van de afscherming van de identiteit van de informant. Dit beschrijft precies de tweede reden waarom informatie niet in de informatiesystemen terechtkomt.

Met betrekking tot (2) het bruto-netto proces waardoor informatie niet in de relevante systemen terechtkomt, constateren wij het volgende. De informatie die na het bruto-nettoën overblijft, is zodanig vervormd en aangepast dat het moeilijker is om het te herleiden tot een specifieke informant. Zo wordt het sociale element van het gesprek dat wel in de bruto-gespreksverslagen staat, niet in de netto-gespreksverslagen opgenomen. En soms wordt informatie vervormd. Indien een informant bijvoorbeeld zegt 'mijn broer Thijs handelt in wapens' dan zal de runner dat veranderen in 'Thijs handelt in wapens'. Het kan dus niet anders dan dat er informatie niet in de systemen terecht komt. Deze informatie kan voor analisten en de productie van intelligenceproducten wel essentieel zijn. Sociale informatie geeft inzicht in de sociale omstandigheden van de informant en de personen over wie hij informatie verstrekt. Voor sociale netwerkanalyses is deze informatie van groot

belang.[255] In BVO-netto is deze informatie echter niet terug te vinden. En de kring van medewerkers die zijn geautoriseerd tot BVO-bruto is zeer klein: slechts een klein aantal analisten heeft toegang tot dit systeem. Voor de meeste analisten geldt dan ook dat deze relevante sociale informatie niet in de voor hen toegankelijke systemen terecht komt.

De laatste door ons gesignaleerde reden (3) betreft een begrip dat in het kennismanagement niet-tastbare kennis (*tacit-knowledge)* wordt genoemd. Deze niet-tastbare kennis laat zich niet in computersystemen opslaan. Niet-tastbare informatie en kennis blijft in veel gevallen buiten de systemen, en indien de CIE en de informatieafdelingen dat willen ontsluiten, zullen ze hiervoor een andere modaliteit moeten verzinnen dan geautomatiseerde systemen. Wij hebben hier nog weinig voorbeelden van gezien. Ad hoc vinden er wel initiatieven plaats waarbij men deze kennis probeert te ontsluiten. Zo vinden er op onderwerpen brainstormsessies plaats met verschillende collega's en in bepaalde gevallen nemen de ervaren CIE-ers de minder ervaren CIE-ers onder hun hoede en dragen ze op die manier kennis over. Van één CIE weten wij dat daar in een korte periode veel ervaren medewerkers met pensioen zullen gaan, en deze medewerkers worden in hun laatste jaar ingezet als een soort adviseurs. Het blijft echter lastig om de niet-tastbare kennis te ontsluiten voor de rest van de organisatie.

C: De informatiesystemen

De grootste inspanningen binnen de politie in het algemeen en IGP in het bijzonder worden gericht op de ICT en de informatiesystemen van de politie. De ICT-ontwikkelingen en de daarbij behorende informatiesystemen vormen een probleem. Dit probleem speelt overigens niet specifiek bij de CIE , maar ook bij de RIO's en de politie in het algemeen.

Alle informatie die door een CIE of een informatieorganisatie wordt verzameld, dient in het BVO-systeem (Basis Voorziening Opsporing) te worden opgeslagen. In het verleden waren er bij de verschillende korpsen honderden systemen in gebruik, hetgeen vandaag de dag steeds verder wordt teruggebracht totdat er één overblijft (zie De Koning 2010; Algemene Rekenkamer 2011). Dit is een belangrijke stap voor IGP en voor de politie in het algemeen, omdat het betekent dat de verschillende korpsen gemakkelijker geautomatiseerd kunnen communiceren en informatie kunnen uitwisselen (dit betreft het onderwerp van sectie 7.6, te weten de verstrekking van informatie en informatieproducten). Specifiek voor de CIE-systemen geldt dat er één landelijke databank wordt ontwikkeld die de onderlinge uitwisseling van CIE-gegevens dient te faciliteren (Klerks 2010: 119). Het huidige systeem is volgens vrijwel alle respondenten echter geen grote vooruitgang voor de verwerking van informatie. Deze mening wordt hieronder ondersteund door een RIO-analist.

"*(BVO) werkt niet goed, is prehistorisch, niet mee te werken en kost zeeën van tijd. Als mensen ernaar kijken, haken ze af.*" Interview analist RIO (A), juli 2007.

Een belangrijke klacht van respondenten over de BVO is dat het niet gebruikersvriendelijk is. Het systeem dateert uit midden jaren '80 van de vorige eeuw

[255] Zie voor een inhoudelijke behandeling van sociale netwerkanalyses: Klerks (2001); Kleemans en De Poot (2008); Morselli (2009); Malm, Bichler en Nash (2011). Wij zullen deze analysemethoden verder niet inhoudelijk behandelen.

en is in veel opzichten erg beperkt in gebruik. Een recherchekundige verwoordt dit als volgt.

"*Alle oude systemen proberen ze nu in één systeem te zetten, dus echt alle systemen die niet eerder met elkaar konden communiceren. Immers, elke regio had een eigen computersysteem, of wel zes eigen systemen waar allemaal informatie in zat. Dat wordt nu langzamerhand in BVO gezet. Dat is ook een heel oud, uit midden jaren '80 stammend systeem. Daar werken we dan nu mee. (…) Het is gewoon heel ouderwets. En de informatie? Vaak zijn er conversies geweest waardoor informatie verloren is gegaan, of informatie is onjuist, er zit oude zooi in die we allang niet meer hadden mogen hebben. Het wordt niet goed geschoond, geen goed onderhoud. Er zitten van sommige subjecten misschien wel meer dan vier persoonskaarten in.*" Interview recherchekundige RIO (B), maart 2011.

Om het doorzoeken van de grote hoeveelheid politie-informatie op een later tijdstip gemakkelijker te maken, dient de invoerder een aantal handelingen verrichten. Het eerste probleem ligt in het aanmaken van kaarten in het systeem waarin bepaalde (persoons-)gegevens worden vastgelegd. Dit wordt in veel gevallen niet goed gedaan. Vervolgens stuiten we op het tweede probleem: het koppelen van deze kaarten aan mutaties. Wanneer er bijvoorbeeld een kaart is aangemaakt voor Thijs Vis, dan krijgt iemand die op die naam zoekt de aan de kaart gekoppelde informatie te zien. De werkwijze van het aanmaken van kaarten en het koppelen van andere mutaties aan die kaarten is echter geen standaardpraktijk. In veel gevallen laten medewerkers het aanmaken van kaarten en koppelen van gegevens achterwege en wordt alleen de informatie ingevoerd. Het probleem hiermee is dat informatie dan erg lastig te achterhalen is: de informatie verdwijnt dan als het ware in de systemen.

Een derde probleem is dat het systeem gevoelig is voor spelling. Indien een naam verkeerd wordt ingevoerd, dan is deze naam slechts te achterhalen indien er gezocht wordt op de verkeerde spelling of indien er op andere zoektermen wordt gezocht die in de bijbehorende mutatie staan. Dit maakt dat er in bepaalde onderzoeken gegevens verloren raken. Er zijn systeembeheerders die een dagtaak hebben aan het aanvullen, verbeteren en opnieuw organiseren van de mutaties in BVO. Vanwege de beperkte functionaliteit van BVO en de gebruikersonvriendelijkheid geven respondenten aan dat het nog steeds niet door alle medewerkers wordt gebruikt. Veel informatie blijft in persoonlijke documenten op de harde schijf van de computer opgeslagen, en deze informatie is niet voor anderen beschikbaar (zie ook de volgende sectie). Hoe groot deze problemen ((1) het niet aanmaken van kaarten, (2) koppelen van informatie, en (3) een onjuiste spelling) zijn, hebben wij niet kunnen vaststellen. Volgens de meeste respondenten is het echter één groot probleem. Een systeembeheerder die als taak heeft om BVO te stroomlijnen verwoordt het als volgt: "*ik word er helemaal gek van, iedereen heeft de opleiding gehad en weet hoe het systeem werkt. Maar eenmaal in de hectiek van de dag lijken ze het allemaal weer te vergeten. Ik ben nu een vliegende keep, mag overal de fouten herstellen. Gek word je ervan.*" (Sociaal gesprek systeembeheerder, medio 2010).

Tijdens een grootschalig onderzoek naar terrorisme hebben wij een aantal keren zelf geconstateerd tot welke problemen de automatisering bij de politie leidt. Tijdens dat onderzoek bleek erg veel informatie in het systeem 'te verdwijnen' omdat er geen kaarten waren aangemaakt, geen koppelingen waren gelegd en er niet goed was ingevoerd. Een gevolg hiervan was dat het achterhalen van relevante informatie een tijdrovende bezigheid werd, terwijl de tijdsdruk in onderzoeken naar terrorisme

enorm is. Op deze manier gaat erg veel tijd verloren aan het zoeken naar informatie. De ICT bij de politie vormt dus niet alleen een barrière tegen de succesvolle implementatie van IGP, maar leidt ook in operationele settings tot problemen, zoals tijdverlies.

7.4.2 Rest- en zijtak-informatie

IGP draait voor een groot deel om het effectief benutten van de in de politieorganisatie aanwezige informatie. Naast de informanten-informatie van de CIE is ook de informatie uit opsporingsonderzoeken van belang bij het verkrijgen van een informatiepositie. Rest- en zijtak-informatie is daarom benoemd als één van de producten van IGP (zie Kop en Klerks 2009: 25). Maar wat is rest- en zijtak-informatie?

"*De andere lijn die in het Zwacri moet komen is de restinformatie. (…) Restinformatie is het dossier minus procesdossier. (…) Die restinformatie moet voldoen aan de criteria van het zwacri. Dat moet eigenlijk ook hierin. Dat noemen ze de zogenaamde 11 informatie.*" Interview analist CIE (F), april 2009.

Rest- en zijtak-informatie is de informatie uit een lopend of afgesloten onderzoek die niet is gebruikt (Van der Bel et al. 2009: 371).[256] Deze informatie kan wel relevant zijn voor het verkrijgen van een beeld van de betrokkenheid van bepaalde personen bij de zware en georganiseerde criminaliteit (de CIE-taak van artikel 10 lid 1 sub a WPG). Het kan worden uitgegeven als start- en sturingsinformatie en als bewijsinformatie. In de praktijk prefereren sommigen overigens de term 'herbruikbare informatie' in plaats van rest- en zijtak-informatie.

Het belang van het gebruik van de rest- en zijtak-informatie wordt al lang door de politie erkend, maar in de praktijk blijkt het bijzonder moeilijk om deze informatie daadwerkelijk bij de belanghebbenden (de CIE, RIO of tactische onderzoeksteams) te krijgen. Hiervoor wordt als reden gesteld dat de politie lijdt aan tijdgebrek. Bovendien heeft het adequaat regelen van rest- en zijtak-informatie geen prioriteit gekregen (zie Kop en Klerks 2009: 60). Onze respondenten onderschrijven dit.

"Een groot probleem is bijvoorbeeld de rest- en zijtak-informatie. Volgens de richtlijnen dienen de tactische teams deze informatie aan ons over te dragen zodat wij het in zwacri kunnen zetten. Wij zijn echter niet in staat om deze bak met informatie te vullen. De plicht ligt echter niet bij ons maar bij tactiek, alleen die krijgen het niet voor elkaar vanwege een gebrek aan capaciteit en dergelijke." Interview hoofd CIE (B), februari 2009

[256] Van der Bel et al. zien restinformatie als informatie uit afgesloten onderzoeken, en zijtak-informatie als een bijzondere vorm van restinformatie die op zichzelf al de mogelijkheid geeft tot het opstarten van een onderzoek (2009: 371). Wij zien echter niet in waarom rest- en zijtak-informatie enkel uit afgesloten onderzoeken afkomstig moet zijn. Het is immers goed denkbaar dat tijdens een lopend onderzoek informatie bekend wordt die betrekking heeft op andere onderzoeken. Deze informatie kan worden overgeheveld naar andere opsporingsonderzoeken (artikel 9 WPG) of de CIE, RID of eenheid belast met een themaverwerking (artikel 10 WPG). Zie de Memorie van Toelichting bij de WPG: *Kamerstukken II*, 2005/06, 30 327, nr. 3, p. 46.

De CIE heeft een specifieke rol bij het verwerken van rest- en zijtak-informatie wanneer het gaat om hergebruik ten behoeve van het verkrijgen van inzicht in de zware en georganiseerde criminaliteit (de CIE-taak, zie subsectie 4.3.2). In de praktijk blijkt de taak die CIE heeft op dit gebied maar lastig uit de verf te komen, en de wijze waarop met rest- en zijtak-informatie wordt omgegaan verschilt per regio. In sommige regio's dient alle informatie uit de opsporingsonderzoeken uiteindelijk overgezet te worden naar het domein van artikel 10 WPG, waarmee het onder de verantwoordelijkheid van de CIE wordt gebracht. In de meeste gevallen hebben de RIO's echter de verantwoordelijkheid over de rest- en zijtak-informatie gekregen. Anno 2012 komt er echter weinig van het hergebruiken van rest- en zijtak-informatie terecht. Een respondent verwoordt het als volgt.

*"(het) gebeurt niet automatisch. Als het onderzoek afgelopen is wordt er niet gelijk een restdossier gebouwd wat eigenlijk aangeboden moet worden aan de officier, die moet er dan voor tekenen om het te kunnen gebruiken, dat het hierin komt. Dit (*artikel 10 lid 1 sub a WPG*) is eigenlijk de bak waar het in moet."* Interview analist CIE (F), april 2009.

Rest- en zijtak-informatie zou een belangrijke bijdrage kunnen leveren aan de analyseproducten op basis waarvan binnen IGP wordt gestuurd omdat het harde informatie is. Informanten-informatie is zachte informatie. Toch wordt er doorgaans meer geïnvesteerd in het breder delen van deze informanten-informatie dan in het hergebruiken van rest- en zijtak-informatie, en dit frustreert een aantal respondenten die bij de CIE werken. In de woorden van een respondent:

"*Wat je ziet is dat we in het verleden veel te veel waarde hebben toegekend aan die (CIE-) informatie ten opzichte van informatie die we opdeden in onderzoeken, tappen, observeren, verhoren. De laatste informatie lekt vaak weg. We maken een dossier op, dat wel, vervolgens vergeten we in de praktijk vaak de rest- en zijtak-informatie goed vast te leggen, dus we verwaarlozen informatie die in werkelijkheid veel betrouwbaarder is omdat we het zelf gehoord hebben, zelf gezien hebben of noem maar op, die uit degelijk recherchewerk naar voren komt of uit andere bronnen te halen is. Die informatie hebben we jarenlang zwaar onderschat, daar hebben we niet veel mee gedaan. Toen hechtten we heel veel waarde aan de informatie van criminelen. Dat moet in balans komen, het is nog steeds hartstikke belangrijk die informatie van de CIE, maar het nieuwe inzicht zal voor het overgrote deel ontstaan op basis van het beter inrichten van je intelligence-organisatie: zorgen dat je goede rest en zijtak hebt, zorgen dat je veel bronnen ontsluit*." Interview hoofd CIE (D), april 2009.

Met betrekking tot de rest- en zijtak-informatie stellen wij vast dat deze informatie nauwelijks de informatiesystemen van de CIE bereikt. De informatiepositie van de politie is versnipperd waardoor bij het opstellen van de analyseproducten die aan de sturing ten grondslag moeten liggen mogelijk relevante informatie wordt gemist.[257]

[257] Heuer (1999) is daarentegen van mening dat meer informatie niet noodzakelijkerwijs ook leidt tot betere analyseproducten. Analisten hebben volgens hem onvoldoende inzicht in de cognitieve processen die aan analyse ten grondslag liggen. De keuzes die de analist maakt zijn minder op daadwerkelijk bewijs (informatie) gebaseerd dan op bepaalde cognitieve vooroordelen. Hij constateert voorts dat een analist slechts een minimum aan informatie nodig heeft voor een adequate analyse. Meer

De sturing vindt daarmee plaats op basis van incomplete informatie, hetgeen de kans op onjuiste beslissingen vergroot.

7.4.3 Tussenconclusies

Met betrekking tot de verwerking van informatie komen wij tot de volgende tussenconclusies c.q. praktijkbevindingen.

Praktijkbevinding 4a: De CIE heeft weinig controlemethoden tot haar beschikking waarmee de betrouwbaarheid van de informant en de informatie kunnen worden beoordeeld. De methoden waarover zij wel beschikt zijn erg arbeidsintensief en tijdrovend. Daarnaast heeft de CIE nauwelijks controle over deze methoden. De CIE-ers die de controle uitvoeren zijn onderhevig aan cognitieve vooroordelen die een objectieve beoordeling erg moeilijk maken. In de praktijk wordt CIE-informatie dan ook vaak (terecht en begrijpelijk) als 'niet te beoordelen' aangemerkt.

Praktijkbevinding 4b: Een deel van de CIE-informatie bereikt de informatiesystemen niet. Dit komt door (1) de tijdsdruk waardoor runners genoodzaakt zijn om samenvattingen in te voeren, (2) het proces van bruto-nettoën waardoor informatie uit het BVO-netto systeem wordt gehouden en (3) het feit dat niet-tastbare kennis niet in systemen kan worden opgenomen. Het in het kader van het strafproces belangrijkste deel van de informatie wordt wel in de informatiesystemen opgeslagen, maar de informatie die niet wordt opgeslagen is vaak voor bepaalde analyses relevant.

Praktijkbevinding 4c: De informatiesystemen waarmee de CIE en de RIO werken kennen zoveel tekortkomingen dat ze een adequate verwerking van informatie belemmeren.

Praktijkbevinding 4d: De informatiepositie van de CIE en de RIO is versnipperd waardoor bij het opstellen van de analyseproducten die aan de sturing ten grondslag moeten liggen mogelijk relevante informatie wordt gemist. Dit komt mede omdat rest- en zijtak-informatie de systemen van de CIE en de RIO niet bereikt.

Concluderend

Op basis van de hierboven geformuleerde praktijkbevindingen komen wij tot de volgende conclusie met betrekking tot het verwerken van informatie. Het op een juiste manier verwerken van informatie is van essentieel belang voor IGP. Het is de basis voor de uiteindelijke informatiepositie van de gehele organisatie. Wij constateren dat de informatiepositie van de CIE te lijden heeft onder (a) tekortschietende mogelijkheden om informatie te beoordelen, (b) falende informatiesystemen en (c) een algemene versnippering van de binnen de politieorganisatie aanwezige informatie. Voor een concept dat uitgaat van informatie als belangrijkste brandstof voor de gehele organisatie, is dit een zorgelijke conclusie.

---

informatie leidt volgens hem tot een onterecht geloof in de eigen inschattingen en een verminderde kritische blik ten aanzien van de eigen analyse en conclusies (Heuer 1999: 52 e.v.).

7.5 Analyse in de praktijk

In deze sectie behandelen wij de acceptatie van de criminaliteitsanalyse bij de politie. Wij maken een onderscheid tussen operationele, tactische en strategische analyse. Operationele en tactische analyse behandelen wij gezamenlijk in subsectie 7.5.1, omdat deze vormen van analyse veel overeenkomsten kennen. Ze zijn beide directer bij het primaire opsporingsproces betrokken dan de meer abstracte, beleidsmatige strategische analyse. De strategische analyse behandelen wij in subsectie 7.5.2. Wij besluiten deze sectie met een theoretische benadering van de door ons gesignaleerde kloof tussen de traditionele recherchefunctie en de nieuwe informatiefunctie, waarin analyse een hoofdrol speelt.

7.5.1 Operationele en tactische analyse

Eén van de bepalende elementen van acceptatie van analyse is dat de verwachtingen van de leidinggevenden (en andere medewerkers van de CIE en de RIO) aansluiten op wat de analisten feitelijk kunnen. Dit betekent dat met name voor de leidinggevenden geldt dat zij duidelijk weten wat de functie van analyse is. Dit geldt ook voor operationele en tactische analyses. Operationele en tactische analisten bereiden de uitvoering van de opsporing voor. Deze vormen van analyse sluiten in theorie goed aan op de traditionele opsporingspraktijk. Bij de CIE betekent dit dat analisten direct betrokken zijn bij specifieke inlichtingentrajecten. Zo verrichten zij informanten-analyses en analyseren zij de gespreksverslagen die door de runners zijn opgesteld. Een typisch analyseproduct van een analist is bijvoorbeeld de beschrijving van een CSV.

De doelstellingen van de operationele en tactische analyse zijn in de praktijk echter nog lang niet altijd duidelijk voor zowel de leidinggevenden als de directe collega's (zoals de runners). De analisten krijgen zelden opdrachten en in de opdrachten die ze wel krijgen, wordt onvoldoende uitgegaan van de kwaliteiten die een analist heeft. Veel respondenten wijzen ons op de gevolgen: onduidelijke opdrachten en analisten die niet weten wat er van ze wordt verwacht. Een recherchekundige brengt dit als volgt onder woorden.

"*Nou, zo'n analist is de eerste tijd bezig met zijn weg te vinden binnen de CIE. Hij komt in een wereld die hij totaal niet kent en moet iets heel nieuws gaan doen. En dan heeft hij misschien wel de opleiding gedaan, maar de theorie is toch wel iets heel anders dan de praktijk, en zeker de CIE-praktijk. Ehm, dus zover zijn we gewoon nog niet. Je ziet aan de andere kant ook dat er vanuit de chefs die de vragen aan de runners moeten stellen geen vragen naar de analisten komen. En zij zitten zo van 'wat moet ik nou in kaart brengen'?*" Interview recherchekundige RIO (B), maart 2011.

In de praktijk worden de analisten belast met het structureren van vrij grote hoeveelheden informatie, doorgaans in een relatieschema. Een deel van de analisten houdt zich bezig met het in kaart brengen van *hotspots, hot crimes, hot times,* en *hot objects.* Om van echte analyse te kunnen spreken, zal een analist naast het structureren van de informatie echter ook moeten interpreteren. Een analist beantwoordt de vraag 'wat betekent datgene wat we zien?' Daarna zal de analist advies uitbrengen (zie Moerland en Mooij 2000). Vaak behelst de analyse in de praktijk echter dat een grote hoeveelheid informatie overzichtelijk in kaart wordt gebracht. Dat wordt door leidinggevenden als voldoende beschouwd. Om echter van

een echte analyse te kunnen spreken moeten de relatieschema's en gegevens worden bewerkt en moet antwoord worden gegeven op de vraag naar wat de betekenis is van de informatie en op welke wijze men dient te handelen. Een relatieschema is meestal een visuele weergave van relevante subjecten en de onderlinge relaties welke worden weergegeven door verschillende lijnen tussen de noden van het netwerk. Er dient een interpretatie plaats te vinden van wat de lijntjes tussen verschillende personen binnen een netwerk eigenlijk betekenen voordat er sprake is van een daadwerkelijke analyse. De interpretatie lijkt er in de praktijk bij in te schieten. Volgens één van de respondenten is de manier waarop de operationele analyse binnen de CIE vorm krijgt 'kinderlijk eenvoudig'.

"*Analisten leren in mijn beleving heel veel plaatjes maken, en poppetjes en figuurtjes. Dat doen mijn kinderen ook. Het gaat er juist om dat je informatie begrijpt, interpreteert, en leest wat er staat. Maar ook leest waarom het er staat. En je moet weten waarom iemand zoiets zegt.*" Interview analist CIE (F), april 2009.

De analyseproducten die wij hebben gezien, zijn volgens ons vaak te kwalificeren als schema's, zoals relatieschema's en overzichten van bewijsposities. En in de praktijk worden analyses doorgaans gelijk gesteld aan presentaties. Wanneer een leidinggevende om een analyse vraagt, bedoelt hij aldus feitelijk een powerpoint-presentatie. Op zich is dat geen probleem, mits er daadwerkelijk een analyseproduct aan de presentatie ten grondslag ligt waarin de analist onder meer kenbaar maakt hoe hij tot zijn analyse is gekomen en waarin hij zijn keuzes verantwoordt. Wij constateren echter dat dit zelden het geval was. Vanwege de tijdsdruk (en het gegeven dat er genoegen mee wordt genomen), beperkte vrijwel alle door ons gesproken analisten zich tot het produceren van powerpoint-presentaties. In andere gevallen was de analyse niet meer dan een advies op een preweeg-document. De leidinggevenden namen genoegen met het advies, zonder dat zij de onderliggende gedachtegang kenden. Toen wij deze leidinggevenden vroegen naar de grondslag voor de adviezen van de analisten, gaven ze aan dat ze uitgingen van de 'eigen kennis en expertise' van de analist en dat ze daarop wel konden vertrouwen. De analisten zelf gaven aan dat ze op de hoogte waren van het feit dat de adviezen geen echte analyses waren, maar dat dit was waar de leiding om vroeg, en "*die willen de adviezen liever gister dan vandaag*".

Volgens enkele respondenten maakte het niet zoveel uit of er daadwerkelijke analyses aan de adviezen en presentaties ten grondslag liggen, omdat de adviezen in veel gevallen alleen werden opgevolgd als ze strookten met de beelden die de leidinggevenden zelf al hadden. Leidinggevenden lijken daarnaast ook van mening te zijn dat de interpretatie van de informatie ook door henzelf, de runners of andere rechercheurs kan worden gedaan. En op zich is deze zienswijze niet onbegrijpelijk. Het werk van de operationele analist lijkt in sommige opzichten namelijk op dat van een rechercheur. Eén respondent verwoordt het als volgt.

"*In principe lijkt een operationeel analist qua denkproces heel erg op een senior rechercheur. Ook de senior rechercheur probeert structuren aan te leggen. In een goed rechercheteam denkt iedereen mee en heeft iedereen een kritische houding. De toegevoegde waarde van een analist is dat hij hoofd- en bijzaken scheidt in de bulkdata. Het denkproces is dus voor beiden gelijk, maar de rechercheur doet ook andere dingen (executief). Wat een operationeel analist precies doet, hangt af van de*

ondersteuning. Veel rechercheurs kennen de basisactiviteiten ook, wellicht geldt dit ook voor de rechercheassistenten." Interview analist RIO (A), juli 2007.

Rechercheurs hebben doorgaans een vergelijkbaar beeld van analisten als de leidinggevenden. De analisten zijn zich hier van bewust. Een analist brengt het als volgt onder woorden.

"*Wat vinden rechercheurs (van analisten)? Zij vinden vooral dat de analist mooie plaatjes maakt. Maar het gaat natuurlijk om een achterliggend denkproces. Wat betekent een plaatje? Dat is de taak van de analist.* " Interview analist CIE (B), juli 2007.

Het komt ook vaak voor dat de uiteindelijke analyseproducten niet worden gebruikt. Wij hebben hierboven al één van de redenen gegeven: als de bevindingen van de analist niet stroken met die van de leidinggevenden, worden ze vaak niet meegenomen in de besluitvorming. Een tweede belangrijke reden is de tijdsdruk waar analisten mee te maken hebben. Vaak worden ze ingehaald door de actualiteit en zijn de bevindingen niet meer nodig voor de besluitvorming. Zo kan het gebeuren dat een analyse wordt aangevraagd op een CSV van een bekende crimineel in het kader van een mogelijk op te starten onderzoek naar de handel in verdovende middelen. Na een week besluit de korpsleiding echter dat overvallen meer aandacht behoeven. Wanneer de analyse is vervaardigd, ook al is men binnen de afgesproken termijn gebleven, blijken de prioriteiten dusdanig veranderd te zijn dat het vervaardigde analyseproduct naar de handel in verdovende middelen aan de kant wordt geschoven om door te gaan met overvallen. Op dit moment ontbreekt concreet zicht op het aantal analyses dat op deze manier in de kast verdwijnt, maar wel is duidelijk dat het de effectiviteit van analysewerk belemmert en eveneens de motivatie van analisten aantast.

In de praktijk lijkt de hiervoor beschreven situatie met betrekking tot de operationele en tactische analyse echter langzaam te veranderen. Zo worden de doelstellingen voor analisten steeds duidelijker geformuleerd en de analisten zelf lijken zich in toenemende mate bewust van de noodzaak voor duidelijke analyseopdrachten. Toch is de analysefunctie binnen de CIE nog steeds duidelijk ondergeschikt aan het verzamelen van informatie. Dit volgt ook uit cijfers omtrent de hoeveelheid analisten binnen de CIE's: gemiddeld is één op de tien CIE medewerkers een analist. De nadruk ligt nog steeds met name op het verzamelen van informatie, en niet op het verwerken en analyseren ervan. Bij de RIO's werken veel meer analisten, maar deze worden verdeeld over de verschillende politieonderdelen. Zo kan een RIO-analist werkzaam zijn bij een zwacri-team of bij de zedenpolitie. Dit maakt dat de verhouding analisten – rechercheurs daar toch enigszins vergelijkbaar is met die van de CIE.

De operationele en tactische analyses worden langzaamaan in toenemende mate geaccepteerd door leidinggevenden en de overige medewerkers. Dit horen wij van de respondenten en hebben wij tijdens het veldwerk geconstateerd. Operationele en tactische analisten worden betrokken bij de verschillende activiteiten en onderzoeken, en operationele en tactische analyseproducten worden ook gebruikt door medewerkers en leidinggevenden. Wij plaatsen hierbij wel een belangrijke kanttekening. Zoals wij hierboven hebben beschreven, is er bij operationele en tactische analyses vaak geen sprake van een 'echte analyse' in de zin dat de voor analyse noodzakelijke interpretatie ontbreekt. Zolang de operationele en tactische analyses zich beperken tot het structureren van grote hoeveelheden informatie, vormt

het geen bedreiging voor de rechercheurs en leidinggevenden. De vraag is echter of de analisten nog steeds worden geaccepteerd wanneer ze zich meer inhoudelijk met het recherchewerk gaan bemoeien en meer gerichte adviezen gaan geven. Een CIE-analist verwoordt het als volgt.

"*Als analist ga je de bruto's beoordelen, en dan ga je allerlei problemen ontdekken die je met ze bespreekt. Maar er zijn weinig runners die dat accepteren. Sommige runners komen naar je toe met allerlei ideeën, die vinden het mooi dat je meedenkt. Dat is geweldig. Maar er zitten een aantal bij die niet mee willen werken, die vinden je maar een zeikerd.*" Interview analist CIE (G), maart 2011.

CIE-analisten die zich op het terrein van de runners begeven en zich inhoudelijk bemoeien met het werk van de runners, krijgen bij wijze van grap toch vaak te horen 'ach wat weet jij nou van het CIE-werk, je hebt nog nooit gerund'. Volgens de runners is dit een grap, volgens de analisten schemert de echte mening van de runners over de analisten er doorheen. Er is binnen de politieorganisatie in het algemeen en bij de CIE in het bijzonder dus sprake van een zekere mate van territoriumafbakening. Een analist die zich begeeft op het territorium van de runners of de leidinggevenden, wordt vaak gezien als een bedreiging en als zodanig behandeld. Hoe dat in de praktijk kan uitpakken, zien we bij het volgende onderwerp: de strategische analyse.

7.5.2 Strategische analyse

De strategische analyse is de meest problematische analysevorm wat de acceptatie door de rest van de organisatie betreft. Het is echter ook de analysevorm die zich bij uitstek leent voor een intelligence-benadering, meer nog dan de operationele en tactische analyse. Dat komt omdat strategische analyse uitgaat van kwalitatieve onderzoeksmethoden, zoals scenario-ontwikkeling en het werken met concurrerende hypotheses. Strategische analyse is in essentie gericht op de toekomst (zie Ratcliffe 2008: 137-138; Ratcliffe 2009; Mc Dowell 2009: 43). De strategische analisten adviseren enerzijds de leiding van de organisatie (het strategisch niveau) omtrent beleidsmatige beslissingen en beleid is per definitie gericht op hoe de organisatie en haar medewerkers in toekomstige situaties dienen te handelen. Het gaat dan om onderzoeken naar trends en ontwikkelingen, CBA's en dreigingsinschattingen zoals het Nationaal Dreigingsbeeld (NDB). Anderzijds kunnen strategische analisten ook operationele leidinggevenden adviseren over de te verwachten gevolgen van bepaalde operationele beslissingen. Dit noemen wij in navolging van Ratcliffe (2009) 'strategisch denken in intelligence'. Onze voorkeur gaat uit naar deze terminologie boven de term 'strategische analyse', omdat de laatste binnen de politie al snel wordt gezien als adviseren op strategisch (beleids-) niveau. Om niet teveel af te wijken van de terminologie zoals die in de politiepraktijk wordt gehanteerd, zullen we echter de term 'strategische analyse' blijven hanteren.[258] Wij willen er nogmaals expliciet op wijzen dat strategische analyse meer omvat dan het adviseren omtrent beleidsaangelegenheden (zie ook Ardon et al. 2011).

[258] Inmiddels wordt er gesproken van 'expert B of C' in plaats van strategisch analist. Dit is het gevolg van een standaardisatie van functies binnen de politie. Het bleek dat er binnen de politie duizenden verschillende functietyperingen waren, en vaak werd dezelfde functie per korps (en zelfs per afdeling) anders genoemd. Dit is inmiddels veranderd: landelijk zijn alle functies gelijk getrokken, hetgeen betekent dat er nu nog ongeveer honderd verschillende functies zijn.

Wij staan uitgebreid stil bij de acceptatie van deze vorm van analyse en behandelen achtereenvolgens (A) het verschil tussen strategische analyse en de traditionele recherche en (B) de manier waarop strategische analyseproducten afwijken van wat men binnen de politieorganisatie gewend is.

A: Het verschil tussen strategische analyse en de traditionele recherche

Het feit dat strategische analyse in een zeker opzicht lijkt op wetenschappelijk onderzoek en dus afwijkt van het referentiekader van de traditionele politiemedewerker is één van de belangrijkste redenen waarom zij nauwelijks wordt geaccepteerd door de medewerkers van de politie, de CIE, en de RIO's daarbij inbegrepen. Omdat leidinggevenden niet weten wat strategische analyse is, weten ze ook niet hoe ze het kunnen gebruiken.

"(…) *Vaak weten ze niet zo goed wat ze met die mensen aanmoeten. Het lijkt soms alsof academici worden gebruikt voor secretariële werkzaamheden, voor het voeden van de stuurgroep. Nou, dat kan een secretaresse ook. Dat is toch doodzonde? Sowieso, academici en politiemensen zijn niet altijd een goede match… Omdat wetenschappers een andere aanpak hebben. Die denken eerst na bijvoorbeeld (lacht). Dat geldt heus niet voor iedereen. Maar politiemensen zijn doeners. Die hebben een doel voor ogen, die bereiken dat linksom of rechtsom… Het zal ook wel vaker voorkomen dat ze iets doen zonder dat ze daar over nadenken. En een wetenschapper zal dat anders doen.* (…)" Interview recherchekundige RIO (B), maart 2011.

Het kan overigens beide kanten op werken: de strategische analist (of andere medewerkers met een academische achtergrond) kunnen op hun beurt ook vraagtekens zetten bij de ervaren rechercheurs.

"*Iemand die al 20 jaar rechercheur is, die ziet een wetenschapper van begin 30, die heeft zoiets van 'wat weet die snotneus nou'? En de wetenschapper, die zal dat misschien wat minder snel uitspreken, maar die denkt misschien 'wat doet die man nou?*'" Interview analist CIE (G), maart 2011.

Er wordt getwijfeld aan het nut van de theoretische kennis van de analist ten opzichte van de operationele ervaring van de rechercheurs. In de woorden van een respondent:

"*Daarnaast was het zo dat de rechercheurs het allemaal wat zweverig vonden, die analyse. Met name toen de tactische en strategische analyse op kwam. Wat gingen wij nou doen wat zij niet konden? Nu maak je dat ook nog wel mee. Bijvoorbeeld met vedomi-onderzoeken* (onderzoeken naar de handel in verdovende middelen, opmerking auteur)*: (…) ze denken dan 'wat weten die strategische analisten daar nou van'? Dat is wel eens vermoeiend*." Interview analist CIE (A), mei 2007.

Het pragmatisme van executieve medewerkers van de politie komt dus niet overeen met de theoretische (vaak wetenschappelijke) benadering van strategische analisten. Dit leidt tot een tweedeling tussen de ervaren rechercheurs en de strategische analisten (en andere medewerkers met een academische achtergrond en zonder uitgebreide recherche-ervaring). Bij de CIE-en zijn overigens weinig strategische analisten in dienst (twee op het moment van schrijven): over het algemeen werken zij bij de RIO's.

Het is niet verwonderlijk dat de rechercheurs en andere medewerkers zich afzetten tegen deze nieuwe zij-instromers en academici die steeds meer in dienst worden genomen. Naast een verschil in achtergrond is er nog een belangrijk verschil: de strategische analist krijgt doorgaans beter betaald dan de andere medewerkers (schaal tien, ten opzichte van schaal zeven of acht voor rechercheurs en operationele analisten en schaal negen voor tactisch analisten). Hier werd herhaaldelijk door respondenten op gewezen.

"Een ander probleem was dat deze functies beter worden betaald dan die van rechercheur, en dat vond natuurlijk geen enkele rechercheur leuk." Interview analist CIE (A), mei 2007.

Een schaal tien-functie staat voor executieve politieambtenaren (politieambtenaren die zijn belast met de uitvoering van de politietaak van artikel 2 Politiewet 1993) gelijk aan de rang van inspecteur (zie artikel 2 lid 1 sub f van het Besluit rangen politie).[259] In de praktijk worden strategische analisten daadwerkelijk vaak door collega's aangesproken op het feit dat ze een hogere schaal hebben. Tijdens een koffiegesprek maakte een rechercheur een keer de volgende grap tegen een strategische analist: "*maak je niet druk als we zeuren over jouw schaal. Je moet weten, politiemensen zijn schaaldieren.*" (sociaal gesprek, december 2010). De hogere schaal gecombineerd met het eerder genoemde verschil in achtergrond (en referentiekader) zorgen ervoor dat de executieve politieambtenaren in de praktijk moeite hebben met het accepteren van de strategisch analisten. Soms wordt dit ook door rechercheurs uitgesproken, aldus een respondent.

"*Tegen mij zeiden ze op mijn eerste werkdag dat ze niet begrepen waarom er weer een strategisch analist was aangenomen. Voor die schaal 10 functie hadden ze ook een paar rechercheurs kunnen aannemen, was de stelling.*" Interview analist CIE (G), maart 2011.

B: De strategische analyseproducten

Een strategische analist verschilt niet alleen qua achtergrond en schaal van de overige medewerkers: ook strategische analyseproducten wijken doorgaans af van de producten waaraan men binnen de politie gewend is. Een typisch (traditioneel) strategisch analyseproduct is de criminaliteitbeeldanalyse (CBA). Dit is een analyse waarbij de aard en omvang van de (georganiseerde) criminaliteit in een bepaald geografisch gebied op een bepaald tijdstip of een bepaalde periode worden beschreven (zie Meesters en Niemeijer 2000: 295). In toenemende mate wordt er in de CBA's overigens ook gekeken naar trends en ontwikkelingen. Een voorbeeld van een ander strategisch analyseproduct is het Nationaal Dreigingsbeeld Georganiseerde Criminaliteit (Klerks 2007: 880).

De belangrijkste verschillen operationele of tactische analyseproducten en strategische analyseproducten betreffen (1) de vorm en (2) de inhoud van de strategische analyses. Hoewel vorm en inhoud in bijna alle gevallen door elkaar lopen behandelen we eerst de vorm. Strategische analyses zijn doorgaans omvangrijke schriftelijke documenten die met name zijn bedoeld om de beleidsmakers van de

[259] Besluit van 25 oktober 1994, houdende vaststelling van regels ten aanzien van de rangen van de politie, Stb. 1994, 792, laatstelijk gewijzigd bij besluit van 27 maart 2011, Stb. 2011, 125.

politieorganisatie te informeren. Ze zijn dan ook vrij abstract, in tegenstelling tot de operationele en tactische analyses, waarbij het vaak gaat om relatieschema's en presentaties die minder omvangrijk en vaak visueel aantrekkelijk zijn. De leidinggevenden wensen daarnaast te beschikken over concrete inzetstrategieën die in de praktijk hun vruchten afwerpen. Die kan een strategische analist niet altijd geven. In de praktijk ligt het zwaartepunt van strategische analyse bij de beleidsadvisering, en niet bij het strategisch denken in operationele setting. Daardoor krijgt de strategische analist weinig mee van wat er op het operationele niveau speelt. Dit is zeker het geval bij strategische analisten bij de RIO's: zij staan doorgaans ver af van het operationele niveau. Strategische analisten die werkzaam zijn bij een CIE hebben doorgaans wel meer zicht op het operationele niveau en kunnen daar een bijdrage aan leveren door bijvoorbeeld (gestructureerde) scenario's te ontwikkelen op basis waarvan beslissingen genomen kunnen worden omtrent aan te lopen informanten.

Het tweede verschil betreft de inhoud van strategische analyseproducten. In tegenstelling tot operationele en tactische analyses bieden strategische analyses vaak weinig ruimte voor eigen interpretatie door rechercheurs en leidinggevenden. Veel leidinggevenden missen ervaring met wetenschappelijk onderzoek en de gebruikte onderzoeksmethoden en zijn daarom niet snel geneigd om inhoudelijk op een strategische analyse in te gaan. In tegenstelling tot de operationele en tactische analisten beperkt de strategische analist in zekere zin de discretionaire ruimte van de leidinggevenden en begeeft hij zich op deze manier wel op het territorium van de rechercheurs en leidinggevenden. Een bepaalde mate van territoriumafbakening is de politie niet vreemd en een dergelijke aantasting van het territorium kan op een tegenreactie rekenen. Inhoudelijk kunnen de rechercheurs en de leidinggevenden echter niet altijd verweer bieden, hetgeen ertoe leidt dat in veel gevallen het instituut van de strategische analyse als zodanig wordt aangevallen. Allereerst worden er vraagtekens gezet bij de nut en noodzaak van strategische analyse en analisten, en vervolgens worden de analyseproducten terzijde gelegd en niet gebruikt bij de besluitvorming. Wij hebben dit laatste met name bijzonder vaak geconstateerd tijdens ons veldwerk: CBA's, dreigingsinschattingen en andere strategische analyseproducten werden nauwelijks gelezen, hoe goed ze ook inhoudelijk zijn. Dit brengt ons tot het derde onderwerp (C): de rol van de strategische analyseproducten bij de besluitvorming.

C: Strategische analyseproducten en besluitvorming

Een gevolg van de bescheiden acceptatie van strategische analyses is dat strategische analyseproducten niet worden gebruikt bij de besluitvorming. Ratcliffe (2008) stelt dat analisten de objectieve stem in de kamer zijn, maar het is ons opgevallen dat zij tevens de zachtste stem zijn. Vaak hebben de leidinggevenden zelf een bepaald beeld van een onderwerp en ze laten zich dan niet of nauwelijks beïnvloeden door analyses. Een recherchekundige zegt hierover het volgende.

"*Eigenlijk wil het MT gewoon zelf beslissen of ze iets willen doen of niet en hebben ze vaak zelf in het hoofd welke kant het op moet gaan. Dan heb je die analyse eigenlijk niet meer nodig. Want dat is toch ook wel ingewikkeld, die analyses kosten veel tijd, het duurt allemaal ook wel lang, we willen toch ook van kant, weet je, we doen het maar.*" Interview recherchekundige RIO (B), maart 2011.

Dit wordt door de analisten ervaren als een belangrijke belemmering van hun werk. De analisten zelf hebben vaak het gevoel dat beslissingen slechts in zeer beperkte mate gebaseerd zijn op analyseproducten. Zo merkten zij op dat zij de indruk hebben dat de jaarlijkse criminaliteitsbeeldanalyses (CBA's) door de leidinggevenden niet worden gelezen, maar dat zij eerder de verkorte (en vereenvoudigde) weergave van de powerpoint-presentatie verkiezen en eigenlijk het liefste geen analyses betrekken bij de besluitvorming. Het algemene beeld is dus dat er van een daadwerkelijke doelgerichte besluitvorming op basis van geanalyseerde informatie geen sprake is. Het is weliswaar op papier wel zo vorm gegeven, maar in de praktijk komt er (te) weinig van terecht. Objectieve besluitvorming op basis van geanalyseerde informatie is echter wel de kern van IGP. Leidinggevenden nemen daarentegen zelf de beslissingen en laten zich nauwelijks leiden door de inzichten van de analisten. Volgens diverse respondenten zijn analisten er met name voor de vorm, en niet voor de inhoud. Een zij-instromer verwoordde het als volgt.

"*(…) Soms, en dat is wel heel negatief gesteld, heb ik het gevoel dat je hier als analyseclub en experts zit voor de vorm, om te kunnen verantwoorden dat je een club hebt voor de analyse. Maar feitelijk zijn de besluiten vaak al genomen. Het is niet op basis van info en het is niet objectief. Ik snap best wel dat op een bepaald niveau belangen spelen die wij niet zien, die wij niet mee kunnen wegen in advisering en analyses, en dat alleen de leidinggevenden dat zien, maar er is ook een ander uiterste. Ik vind dat we het nu gewoon niet goed doen. Dat is aan het management te wijten. Misschien is het ook wel vertrouwen, misschien vertrouwen ze de werkvloer niet dat het goed komt.*" Interview recherchekundige RIO (A), mei 2010.

De ondergeschikte rol van analyse bij de besluitvorming heeft ook te maken met een verschil in informatiepositie tussen de leidinggevende en de analist. Vanwege (1) de huidige structuur van de informatiehuishouding, waarbij de hoogte van de autorisatie primair afhangt van de hoogte van de functie, en (2) de informele informatienetwerken waarvan met name de leidinggevenden deel uitmaken (zie sectie 7.5), zijn er bepaalde leidinggevenden die uiteindelijk over de meest relevante (kwalitatieve) informatie beschikken. Dit hebben wij met name bij de RIO's gezien. Formeel hebben de betreffende leidinggevenden ook de toegang tot de meeste informatie. De analisten van de RIO (en overigens ook veel analisten binnen de CIE) analyseren de 4*3-tjes, de netto-informatie dus. Doorgaans gaat het om informatie met de code 11. In sommige gevallen krijgen zij 01 informatie te zien en in uitzonderlijke gevallen 00, 200 en 300 informatie. Dat laatste is echter niet de norm: dit is voorbehouden aan de CIE-analisten, en ook zij krijgen niet altijd alle informatie te zien. De analist mist dus altijd bepaalde informatie die relevant kan zijn. De leidinggevende beschikt doorgaans over meer informatie of krijgt deze informatie op een eerder moment.[260] Voorts kan het ook zijn dat de leidinggevende een informatievoorsprong heeft op de analisten door informatie via informele netwerken: de leidinggevende wordt doorgaans als eerste gebeld of anderszins in kennis gesteld van relevante nieuwe informatie. Een oplossing voor dit probleem zou een uitbreiding van vertrouwen kunnen zijn door de analist te autoriseren voor de 01, 00, 200 en 300 informatie. Maar dit zou niet onze oplossing zijn. Wij zouden eerst een kwalitatieve inventarisering via leidinggevenden willen voorstellen. Op grond daarvan kan een

[260] Dit kan overigens belangrijke consequenties voor de inhoudelijke kwaliteit van de analyses hebben. De kwaliteit van analyses valt echter buiten het bereik van ons onderzoek.

beter oordeel worden gevormd over de aard en omvang van deze problematiek. Daarbij is het wel zo dat de analisten doorgaans op de hoogte zouden moeten zijn van de meeste informatie omdat het hun taak is om de informatie te interpreteren. Zij hebben in theorie een kwantitatieve informatievoorsprong op leidinggevenden welke ze in bepaalde gevallen ook kunnen gebruiken om de sturing te beïnvloeden. Tijdens ons veldwerk bleek dat er echter altijd leidinggevenden zijn die beschikken over een kwalitatieve informatievoorsprong. Zij weten net wat meer over de aspecten die de daadwerkelijke besluitvorming kunnen beïnvloeden, of zij doen het voorkomen alsof ze meer weten. Dat maakt dat zij vaak beslissingen nemen die in de ogen van de werkvloer niet zijn gebaseerd op objectieve informatie (analyses) en daarmee soms onbegrijpelijk zijn. Dit hebben wij een aantal keren geobserveerd op de werkvloer. Een genuanceerd voorbeeld zegt soms meer dan een algemene analyse, hoewel we juist met zo'n redenering voorzichtig moeten zijn. Wij geven toch een voorbeeld, dat laat zien hoe we tot onze bevindingen zijn gekomen. In één geval kreeg een analist de opdracht om een preweegdocument te beoordelen en te controleren of het voldeed aan de doelstellingen die de stuurploeg had vastgesteld. Hij kreeg de opdracht op een donderdag en had een week de tijd om advies uit te brengen. Een dag voordat de stuurploeg bij elkaar kwam om het product te beoordelen, moest hij het doorspreken met een leidinggevende die deel uitmaakt van de stuurploeg. De leidinggevende bleek over cruciale informatie te beschikken uit het buitenland en paste het advies op grond daarvan inhoudelijk aan. Eigenlijk was de analyse helemaal niet nodig geweest voor de uiteindelijke beslissing, dit tot frustratie van de betreffende analist. Volgens diverse analisten gebeurt dit erg vaak. Het is echter ook een gevolg van de rol van een analist: de analist adviseert, maar neemt geen sturingsbeslissingen. En in die gevallen dat een leidinggevende over relevante informatie beschikt die tot een beslissing leidt die van het advies van de analist afwijkt, is dat misschien vervelend voor de analist maar desalniettemin legitiem. Het kan echter ook zijn dat een leidinggevende een bepaald beeld heeft dat is gevormd door bepaalde subjectieve ervaringen en dat afwijkt van de resultaten van analyse. Beslissingen die dan afwijken van de adviezen van de analist zijn een stuk minder legitiem.[261] Of de beslissing legitiem is of niet, is overigens doorgaans bijna niet te beoordelen. Wij kunnen dat in ieder geval niet.

Wij sluiten af met de vaststelling dat de strategische analyse nauwelijks wordt geaccepteerd door de leidinggevenden. Leidinggevenden weten niet zo goed wat ze met strategische analisten aan moeten. Dit verklaart ook voor een deel waarom de analyseproducten niet worden gebruikt bij de besluitvorming: onbekend maakt onbemind. Wij constateren dat de strategische analyse om drie redenen niet wordt geaccepteerd: (1) de strategisch analist is hoger opgeleid dan de leidinggevende, (2) de strategisch analist zit in een (relatief) hoge schaal ten opzichte van de rechercheur en (3) strategische analyseproducten wijken af van wat men binnen de politieorganisatie gewend danwel wat gewenst is.

[261] Het hier geschetste beeld moet enigszins worden gerelativeerd. Veel leidinggevenden geven aan dat zij de analyses grondig scannen en de managementsamenvatting lezen. Volgens hen spelen de presentaties door analisten tijdens managementoverleg wel degelijk een rol bij de besluitvorming. Omdat wij dergelijke bijeenkomsten niet mochten bijwonen, kunnen we echter niet zeggen in welke mate de besluitvorming daadwerkelijk wordt gebaseerd op het werk van de analisten. Feit is wel dat andere factoren, zoals overwegingen over media-aandacht en beschikbare capaciteit, ook een belangrijke rol (kunnen) spelen bij het nemen van beslissingen. Wij hebben echter tijdens het veldwerk geconstateerd dat in een stuurgroep-overleg de adviezen van de analisten worden gepresenteerd en toegelicht door de leidinggevende van de analisten, en niet door de analisten zelf. Dit leidt volgens de analisten vaak tot een onbedoelde aanpassing van de conclusie van de analyse, of er wordt op de verkeerde bevindingen een accent gelegd.

7.5.3 De traditionele recherchefunctie versus de nieuwe informatiefunctie

'Informatie' wordt in toenemende mate gezien als een zelfstandig specialisme. Het is geworden tot een expertise naast de traditionele recherche en het CIE-werk. Dit kan het negatieve neveneffect kan hebben dat de afstand tussen de analisten en rechercheurs groter wordt. Het accent van het politiewerk verschuift van de traditionele recherchewerkzaamheden die zich 'op straat' afspelen naar informatie-gerelateerde werkzaamheden die zich veel meer achter het bureau en het beeldscherm afspelen (zie ook Van der Torre 2007: 516; Van Calster et al. 2010 (a): 186). De afstand tussen analyse en de praktijk van het recherchewerk (inclusief de CIE) wordt in veel regio's groter door de invoering van RIO's. De RIO's zijn als het ware de belichaming van de nieuwe informatiefunctie, en worden door de traditionele rechercheafdelingen dan ook met argwaan aanschouwd. De RIO's vervullen een rol met betrekking tot de informatiefunctie die de CIE-en en de tactische opsporingsteams hebben laten liggen. Dit leidt echter tot concurrentie tussen de verschillende afdelingen. Een teamleider zei hierover het volgende.

"*Om in markttermen te spreken: er was een markt die niet benut werd. En anderen zagen daar ruimte om die wel te benutten. Er is behoefte aan, er is een markt voor, dus laten we dat maar gaan doen. En daar ontstaat een zekere strijd tussen de afdelingen die de markt inpakken die eigenlijk bij de CIE hoort maar die de CIE niet zelf oppikt, door capaciteitsproblemen ofzo. Je ziet ook een zekere verschuiving van de macht van CIE naar de recherchechefs (…).*" Interview teamleider CIE (D), november 2009.

De vraag is nu hoe er vanuit de CIE naar de RIO wordt gekeken. Wij nemen tijdens ons veldwerk duidelijk een concurrentiestrijd tussen de CIE en de RIO waar. Zo worden wij herhaaldelijk gewezen op de tekortkomingen van de RIO's: "*die lui weten helemaal niks, ze snappen er niks van. Wat zitten ze nou de hele dag te doen?*" (sociaal gesprek met een tactisch rechercheur, december 2010). Een leidinggevende verwoordt het als volgt: "*met een RIO is nog nooit een boef gevangen.*" (sociaal gesprek met een leidinggevende, mei 2009). Deze concurrentie tussen de CIE en de RIO wordt versterkt door het proces van sociale categorisatie, een proces dat wij hieronder zullen toelichten.

Het verdelen van de wereld in 'wij versus zij' is een sociaal proces, dat in de psychologie 'sociale categorisatie' wordt genoemd (zie Baron, Byrne en Johnson 1998).[262] Eenvoudig geformuleerd leidt sociale categorisatie ertoe dat de personen in een zogeheten *ingroup* ('wij') positief worden bekeken, terwijl personen die tot een *outgroup* behoren ('zij') negatieve(re) eigenschappen krijgen toebedeeld (zie ook: Brown 2001: 497-500). Deze scheiding tussen een *ingroup* en een *outgroup* leidt binnen de *ingroup* tot versterkte saamhorigheid, waarbij onderling sterke gevoelens van solidariteit en loyaliteit heersen (Baron et al. 1998; Brown 2001: 498).

Sociale categorisatie vindt bij de politie zowel extern als intern plaats. Bij de politie heersen saamhorigheid, solidariteit en loyaliteit erg sterk: er is sprake van een sterk wij/zij perspectief (Van der Torre 2007: 497-498). En dat is niet verwonderlijk. Immers, om het (niet zelden gevaarlijke) werk zo effectief en veilig mogelijk uit te voeren, is een goede samenwerking van groot belang (Westwood 2001). Men moet

[262] Zie voor een artikel over IGP en sociale categorisatie waarvan wij co-auteurs waren: Van Calster, et al. (2010).

zijn collega's onvoorwaardelijk kunnen vertrouwen. Dit zorgt voor een externe sociale categorisatie, waarbij de politie tegenover de rest van de samenleving staat. Dezelfde dynamiek van sociale categorisatie vindt ook intern, binnen de politie, plaats. In dit hoofdstuk is deze interne sociale categorisatie van groter belang dan de externe sociale categorisatie. Binnen de politie bestaat een indeling in subculturen, die voortkomt uit de hoeveelheid aan verschillende afdelingen, eenheden, en teams met ieder hun eigen taak (zie Punch et al. 1999). Door de intensieve samenwerking ontstaat ook binnen de afdelingen en eenheden een bepaalde vorm van saamhorigheid. Dat kan ertoe leiden dat men zich afzet tegen de andere afdelingen of eenheden. En dit heeft dan weer negatieve gevolgen voor de interne samenwerking: de concurrentie tussen de afdelingen neemt hierdoor toe.

De sociale categorisatie en de tweedeling tussen de recherche- en informatiefunctie blijken onder meer uit een verschil in waardering tussen politie- en burgerwerk. Uit de gegevens die ons ter beschikking staan (zie hoofdstuk zes) blijkt dat er door sommigen in de praktijk vaak een onderscheid wordt gemaakt tussen 'echt politiewerk' (boeven vangen) en 'bureauwerk' (bijvoorbeeld analyse). Wij hebben de indruk dat binnen de Nederlandse politie het beeld levend wordt gehouden dat rechercheurs door 'boevenvangen' het 'echte werk' doen (zie ook: Cope 2004). Het feit dat sommige executieven de mening zijn toegedaan dat zij zeer capabel zijn om het analysewerk zelf uit te voeren, wijst eveneens in die richting: 'wij vangen boeven en doen het analysewerk erbij'. Het kan ook duiden op een gevoel van een zekere mate van onderwaardering van de analisten en hun werk. Uit ons onderzoek blijkt overigens dat deze onderwaardering (zo zij al zou bestaan) het meest zichtbaar lijkt op lokaal niveau, te weten de districten en wijken (zie Van Calster et al. 2010). Wellicht zetten de politiemensen zich daar het meest af tegen het voor hen onzichtbare analysewerk vanwege hun fysieke en mentale afstand: de meeste analisten die zich bezighouden met georganiseerde criminaliteit werken op regionaal niveau. Voorts kan het zijn dat de doelstellingen van analyse in groter contrast staan met de doelstellingen van het werk op lokaal niveau. Het werk op lokaal niveau, waar vaak direct criminelen van straat worden gehaald, kan op grond daarvan als 'belangrijker' worden beschouwd dan het werk op regionaal niveau, waar vaak meer indirect (en misschien wat abstracter) wordt bijgedragen aan de veiligheid op straat (zie ook: Van Calster et al. 2010 (a): 185-186). Hiermee wordt overigens wel het contrast tussen *ingroup* (wijken en districten) en *outgroup* (analisten) aangescherpt. Daarnaast wordt het werk op regionaal niveau vaak gezien als 'saai en minder belangrijk kantoorwerk', en het werk op lokaal niveau – de directe praktijk – lijkt te worden gezien als het 'echte werk'. Dit onderscheid speelt ook tussen het regionale en het nationale niveau. Wij hebben tijdens ons veldwerk vastgesteld dat de (georganiseerde) criminaliteit voor analisten op landelijk niveau vaak abstract is. Het is een papieren realiteit. Analisten in de regio's zitten vaak dichter op de criminaliteit zelf. Voor de regionale analisten is het gemakkelijker om ook daadwerkelijk de straat op te gaan en een gevoel te krijgen voor de subjecten, fenomenen of groeperingen waar zij analyses van maken. Hoe verder we in de politieorganisatie afdalen, des te gemakkelijker wordt het dit onderscheid voort te zetten. Andersom zullen de analisten die werkzaam zijn bij landelijke eenheden op hun beurt beschikken over een groter overzicht en verbanden tussen informatie afkomstig uit verschillende regio's. De sociale categorisatie kan dus ook de andere kant op werken: landelijke analisten die zichzelf boven regionale analisten plaatsen vanwege een (vermeende) informatievoorsprong.

Een aantal jaren terug (tot begin 2000) speelde de kloof tussen analyse en het recherchewerk zich echter veel meer aan de oppervlakte af dan vandaag de dag (2012) het geval is. Een analist verwoordt het als volgt.

"*Vroeger werden analisten gezien als de geitenwollensokken types. Toen werd je gewoon niet geaccepteerd. Dat had meerdere redenen. Allereerst waren veel van de analisten destijds ook een beetje contactgestoord. Erg slim maar moeilijk in de omgang. Daarnaast was het zo dat de rechercheurs het allemaal wat zweverig vonden, die analyse. Een andere belangrijke reden voor de zwakke positie van de analist in het begin was dat wanneer een rechercheur z'n been brak, hij een bureau aanstelling kreeg. Dat was dan analist. (…) Nu is het veel beter, ze merken dat wij wel degelijk een overzicht hebben. Daarnaast gebruiken we analist notebook, wat leuke plaatjes oplevert en daar houden ze hier van.*" Interview analist CIE (B), mei 2007.

Wij zien de kloof tussen de recherchefunctie en de informatiefunctie het duidelijkst wanneer het de strategische analyse betreft. Strategische analyse is nu eenmaal het verst verwijderd van het traditionele recherche- en CIE-werk. De operationele en tactische analyse worden zoals gezegd min of meer geaccepteerd als aanvulling; ze vormen geen inhoudelijke bedreiging voor de rechercheurs en het leidinggevende kader. De strategische analyse speelt eigenlijk dezelfde rol maar dat wordt (nog?) niet zo gezien.

Wij sluiten deze subsectie af met de opmerking dat het onderscheid tussen een recherche- en een informatiefunctie ons bevreemdt. 'Informatie' is geen op zichzelf staande expertise: het is binnen de opsporing noodzakelijkerwijs verbonden met het primaire rechercheproces. Het loskoppelen van de recherchefunctie van de informatiefunctie komt voort uit de illusie dat het hier om twee verschillende functies (en expertises) gaat. Het mogelijke gevolg van de tweedeling tussen de traditionele recherchefunctie en de 'nieuwe' informatiefunctie is een onderlinge concurrentie tussen de afdelingen die een taak hebben op het gebied van de bestrijding van de georganiseerde criminaliteit. Wij zijn dan ook van mening dat de tweedeling mogelijk zal leiden tot een verzwakking van beide functies, en men zou er in dit opzicht beter aan doen om de functies te integreren en te zien als een onderdeel van hetzelfde proces: de bestrijding van de georganiseerde criminaliteit en het terrorisme. In dit opzicht sluiten we ons tot slot aan bij de signalering van Fijnaut (2010: 17): "*(…) als gevolg van de op zich al vrij idiote theorie van informatiegestuurd politiewerk, maar vooral van het daarbij behorende heilige geloof in intelligence als ware het manna (is er sprake van) zo'n absurde tweedeling tussen opsporing en informatie dat goede rechercheurs er wanhopig van worden en met recht en reden omwegen zoeken (…) om de 'natuurlijke' samenhang tussen deze beide dingen weer enigszins te herstellen.*"[263]

7.5.4 Tussenconclusies

Met betrekking tot de criminaliteitsanalyse komen wij tot de volgende tussenconclusies, ook praktijkbevindingen genoemd.

[263] Wij zijn het (uiteraard) niet eens met de kwalificatie 'idiote theorie' wanneer Fijnaut over IGP spreekt. De theorie heeft onzes inziens zeker een toegevoegde waarde voor de praktijk van de CIE en de RIO (en de recherche in het algemeen).

Praktijkbevinding 5a: De operationele en tactische analyse is ingeburgerd in de praktijk van de CIE en de RIO's.

Praktijkbevinding 5b: Operationele en tactische analisten worden in de praktijk met name belast met het structureren van grote hoeveelheden informatie. Van een interpretatie van de gestructureerde informatie is doorgaans in mindere mate sprake.

Praktijkbevinding 5c: Strategische analyse is nauwelijks ingeburgerd in de praktijk van de CIE en de RIO's. Dit komt met name omdat de strategische analyses afwijken van het referentiekader van de traditionele politiemedewerkers. Daarnaast laat de strategische analyse weinig ruimte over aan de leidinggevenden om zelf de informatie te interpreteren.

Praktijkbevinding 5d: In de praktijk is er een kloof tussen de traditionele recherchefunctie en de nieuwe informatiefunctie. Dit leidt tot onderlinge concurrentie, hetgeen wordt versterkt door interne sociale categorisatie.

Concluderend

Op basis van de hierboven geformuleerde praktijkbevindingen komen wij tot de volgende conclusie. Anno 2012 is criminaliteitsanalyse nog steeds geen vanzelfsprekend onderdeel van de politieorganisatie. Dit geldt met name voor de strategische criminaliteitsanalyse, welke nauwelijks wordt gebruikt bij het ontwikkelen en formuleren van beleid. Dat is niet goed voor de implementatie van IGP, omdat strategische criminaliteitsanalyse uitgaat van een van lange-termijn-beslissingen. De traditionele recherchefunctie (waar de traditionele CIE deel van uitmaakt) en de informatiefunctie hebben een onderlinge concurrentie. De concurrentie tussen deze twee functies maakt de afstand tussen aan de ene kant het verzamelen en aan de andere kant het analyseren van informatie steeds groter. IGP gaat uit van de verbinding tussen het sturen op informatie (de traditionele recherchefunctie) en het sturen met informatie (de informatiefunctie). De huidige situatie is dus potentieel rampzalig. Zonder een verbinding en afstemming tussen deze twee functies kan er niet worden gesproken van IGP.

7.6 Verstrekken in de praktijk: de intra-organisatorische geheimhouding

In deze sectie behandelen wij het verstrekken van informatie door de CIE. Verstrekkingen zijn nauw verbonden met geheimhouding, en geheimhouding is een essentieel onderdeel van het CIE-werk. IGP gaat echter uit van het maximaal delen van informatie, oftewel: de *need to share*.

In deze sectie behandelen wij de spanning tussen de geheimhouding en het streven naar *need to share*. Het gaat hier om de politie-interne geheimhouding. Eerder hebben we dit het intra-organisatorisch perspectief genoemd (zie subsectie 2.6.1). In hoofdstuk vijf hebben wij de tweeledige doelstelling van het NIM met betrekking tot *need to share* geformuleerd: ten eerste moet de onnodige geheimhouding worden doorbroken en ten tweede moet de informatie-uitwisseling die plaatsvindt via de *old boys networks* worden geformaliseerd en geïnstitutionaliseerd (subsectie 5.6.2).

Wij beantwoorden de vraag waarom het NIM er anno 2012 nog niet in is geslaagd om de geheimhouding te doorbreken in subsectie 7.6.1. Wij richten ons in deze subsectie op de CIE en laten de RIO grotendeels buiten beschouwing, omdat de

RIO eigenlijk zelf nauwelijks informatie verzamelt maar voor haar informatievoorziening met name afhankelijk is van de CIE en de tactische opsporingsteams. De informatie die de RIO verzamelt is eerder door andere organisatieonderdelen verzameld: de RIO richt zich met name op de interne informatiestromen. De te doorbreken geheimhouding speelt dan ook met name bij de CIE en de tactische opsporingsteams. De tactische opsporingsteams vallen echter buiten het bereik van ons onderzoek. Vandaar dat wij ons tot de CIE beperken. Vervolgens behandelen wij in subsectie 7.6.2 in hoeverre het NIM in staat is gebleken om de tweede doelstelling van *need to share* te bereiken: het institutionaliseren en formaliseren van de informele informatiestromen, oftewel de *old boys networks*.

7.6.1 Doelstelling 1: *Need to share* bij de CIE

Het is evident dat het delen van informatie van groot belang is voor de opsporing in het algemeen en IGP in het bijzonder. De premisse van *need to share* is dat er in de praktijk (veel) minder informatie wordt gedeeld dan mogelijk is en dat dit komt vanwege een *need to know* cultuur (NIM 2008; zie ook subsectie 5.5.2). De gedachte binnen een groot deel van de politie lijkt te zijn dat deze cultuur moet worden doorbroken. Wij bezien in deze subsectie in hoeverre dit is gelukt bij de CIE. Daartoe bezien we allereerst (A) in hoeverre de medewerkers van de CIE het *need to share* streven onderschrijven. Vervolgens behandelen wij (B) de gevaren die *need to share* volgens CIE-ers met zich meebrengt. Hierna gaan wij in op (C) de verschillende manieren waarop CIE-ers verzet plegen tegen de invoering van *need to share*. Wij sluiten de subsectie af met (D) een antwoord op de vraag waarom de implementatie van *need to share* binnen de CIE vooralsnog niet is gelukt.

A: In hoeverre onderschrijven CIE-ers need to share?

Een antwoord op de vraag in hoeverre CIE-ers de *need to share* onderschrijven, is niet makkelijk te geven. CIE-ers zijn zelf doorgaans van mening dat zij maximaal informatie delen met anderen. Over het algemeen geven de meeste respondenten in eerste instantie aan dat zij het *need to share* streven onderschrijven. Volgens veel CIE-ers zijn zij de laatste jaren veel meer informatie gaan delen, met name als CIE-en onderling. Een respondent, die tijdens het interview voor de RIO werkte maar die in het verleden bij de CIE heeft gewerkt, omschreef de situatie als volgt.

"*Het is de laatste jaren zo dat CIE-en onderling wel informatie met elkaar delen. In ieder geval die informatie die volgens de wet gedeeld mag worden. Dus dat is niet het probleem. Het is zelfs zo dat is afgesproken dat we de informatie op 00 niveau delen met alle medewerkers. Dat is zeker gezien de geschiedenis best bijzonder. En waarom dat vertrouwen is gegroeid is omdat we weten van elkaar dat mensen binnen de CIE weten hoe er met die informatie moet worden omgegaan. Dat schept vertrouwen en dat zit wel goed. Het (probleem) zit meer daar waar het het CIE-domein overschrijdt.*" Interview recherchekundige RIO (B), maart 2011.[264]

Dezelfde CIE-ers geven echter ook aan dat geheimhouding inherent is aan het inlichtingenwerk. Dat sommige informatie niet wordt gedeeld, heeft volgens CIE-ers met name te maken met afschermingsbelangen. Zij wijzen met name op de

[264] Deze respondent heeft in het verleden bij de CIE gewerkt.

operationele redenen voor geheimhouding (zie subsectie 2.6.2). Maar zij zijn van mening dat ze alles delen voor zover de afscherming van de identiteit van informanten dat toestaat. Een hoofd CIE zei hierover het volgende.

"*Het uitgangspunt is: in principe delen wij alles, zolang de identiteit van de informant niet in het geding is.*" Interview hoofd CIE (B), februari 2009.

Het delen van meer informatie dan de afscherming toestaat is volgens de respondenten van de CIE onverantwoordelijk en leidt tot grote gevaren voor de informanten. Maar binnen de CIE is men doorgaans van mening dat men maximaal informatie deelt met anderen.

Medewerkers van de RIO's (en overige rechercheonderdelen) zijn echter een andere mening toegedaan. Zij geven aan dat de CIE nog meer zou moeten delen dan zij nu doet. Volgens deze medewerkers speelt het afschermingsbelang minder sterk dan de CIE stelt, en liggen er vaak andere oorzaken aan de geheimhouding ten grondslag. Zij geven aan dat de CIE 'op de informatie blijft zitten' vanwege een te ver doorgevoerde geheimhouding. Van daadwerkelijke bronbescherming zou volgens hen niet in alle gevallen sprake zijn; de reden voor geheimhouding zou ook vaak liggen in de 'kennis is macht'-redenering of het afschermen van een tekortschietende informatiepositie. In de woorden van een respondent luidt deze redering als volgt.

"*(…) mijn indruk is wel dat men om je eigen waarde te behouden informatie bij zich houdt. Zo van 'ik ben expert op dit onderwerp en ik heb goede één op één lijntjes (want daarvan is ook veel afhankelijk, hoe je contacten zijn binnen andere regio's)'. En wanneer je de informatie gaat delen met andere dan raak je die positie een beetje kwijt. Dan ben je niet meer zo uniek of waardevol voor de organisatie (...). Kennis is zeker macht.*" Interview recherchekundige RIO (A), mei 2010.

Andere respondenten relativeren de noodzaak van geheimhouding en de afschermingsbelangen.

"*(…) er moet een awareness komen (…) dat je heel goed kijkt hoe groot is dat afschermingsbelang nu op zichzelf en is het in zijn aard ook zo exclusief als dat we dachten. Binnen de CIE waar dat afschermingsbelang nog gevoeld wordt, moet heel goed bekeken worden: wat is er in de rest van het bedrijf al bekend. Misschien blijkt dat die informatie er al was of voor een deel al was. Dan kun je over dat deel in ieder geval open communiceren, dan wel dat je vanuit het totale spectrum gaat kijken is ok, dat is eigenlijk hetzelfde verhaal. Door het in ieder geval te toetsen het maximaal terugleggen; dat gebeurt ook door het te spiegelen aan wat we voor de rest al weten. Nu gaat het anders, nu zie je dat de CIE nog een redelijk autonome entiteit is, die zijn informatie binnenhaalt, zijn informatie vastlegt en vervolgens kijkt of ze af en toe een pv of een informatierapport bij de recherche neerleggen, dus het is maar éénrichtingsverkeer.*" Interview teamleider RIO (C), april 2009.

Een andere respondent stelt hieromtrent het volgende.

"*Informatie van een politieman dient altijd gedeeld te worden, omdat de bron niet met het individu praat, maar met de politieorganisatie. Dit staat los van de CIE, maar ook voor de CIE geldt dat binnen de CIE-en een dergelijk gegeven bestaat. Alle informatie moet gebruikt worden en om dit op een acceptabele wijze te doen kan je*

bijvoorbeeld een status aan bepaalde informatie hangen. Maar iedereen die een CIE-status heeft, moet alles weten wat er binnen de CIE ligt, inclusief de bronverslagen." Interview analist RIO (A), juli 2007.

Er is dus sprake van een verschil van inzicht tussen de CIE en de informatieafdeling. De medewerkers van de RIO willen de CIE-informatie inzien, inclusief de 00, 200 en 300 informatie. Volgens enkele respondenten komt dit met name voort uit een soort informatiehebzucht van niet-CIE-ers.

"*Het is allemaal het idee dat je zoveel mogelijk informatie moet kunnen hebben. Hebben, hebben, hebben. Maar aan wat je mag weten en wat je mag zien zijn gewoon beperkingen gebonden. Dus dat heeft als gevolg dat bepaalde mensen bepaalde informatie niet mogen zien omdat ze dat niet nodig hebben voor hun taak of omdat het privacy-technisch niet handig is. Dan moet je dat dus niet willen. Maar dat vinden mensen vervelend, want waarom mag hij dat wel weten en ik niet? We zijn toch vrienden? Waarom weet iemand die bij de CIE zit meer dan ik die niet bij de CIE zit? En waarom mag ik niet door alle lopende onderzoeken heen kijken, dat is toch hartstikke handig? Gooi het allemaal maar op een stapel en dan vallen vanzelf wel de grote boeven eruit.*" Interview recherchekundige RIO (A), mei 2010.

De CIE-ers zijn op hun beurt van mening dat zij zelf het beste kunnen bepalen wat veilig is om te delen. Dat coderen ze met 11 en 01, en dat is de informatie waarmee de medewerkers van de RIO kunnen werken. CIE-ers zetten daarnaast op hun beurt vraagtekens bij de suggestie dat geheimhouding primair een CIE-aangelegenheid is. Ook andere onderdelen van de politie zouden geheimhouding betrachten. In de woorden van een hoofd CIE is de situatie als volgt.

"*De cultuur van niet willen delen wat voorheen werd gezien als specifiek iets voor de CIE is iets van vroeger. Zoals gezegd willen wij ook meedelen in het succes: ook wij willen boeven vangen. Ook de vaak veronderstelde culturele eigenschap dat men informatie voor zichzelf wenst te houden is meer iets van vroeger. Dit is ook niet specifiek iets voor de politie, maar is menselijk. Zet maar eens een paar programmamakers bij elkaar, die gaan ook niet alle goede ideeën direct met elkaar delen. Het besef van de noodzaak om informatie te delen is er de laatste jaren door de aandacht ervoor wel doorgedrongen.*" Interview hoofd CIE (B), februari 2009.

De CIE verwijt de tactische teams echter dat juist ook zij teveel informatie afschermen, en klaagt bijvoorbeeld over het wijdverspreide gebruik van embargo-onderzoeken waarmee veel informatie uit die onderzoeken voor de CIE afgeschermd blijft. Dit zouden ze volgens medewerkers van de CIE uit rancune doen omdat ze niet alle CIE-informatie verstrekt krijgen. In de woorden van een CIE-er.

"*Er blijkt in de praktijk dat er steeds meer embargo-onderzoeken zijn, en daarvan kan ik niks zien, de tekst niet, de entiteiten niet, helemaal niks. Dit is best een groot probleem. We kunnen als CIE niet bij tientallen onderzoeken, waardoor we relevante informatie gaan missen. Een deel van de leiding wil niks delen, zeker niet met de CIE. Ze willen alles voor zichzelf houden.*" Interview analist CIE (G), maart 2011.

Waar vrijwel alle respondenten het over eens zijn, is dat er sprake is van een cultuur van geheimhouding. De premisse van het NIM dat de cultuur van geheimhouding

voortkomt uit een oneigenlijk of onnodig gebruik van het *need to know* denken, kunnen wij niet bevestigen of ontkrachten. Geheimhouding wordt immers volgens beide 'partijen' oneigenlijk gebruikt, en wij kunnen niet beoordelen of deze claims op waarheid berusten. Wat wij wel kunnen vaststellen is dat wanneer een partij, ongeacht of dit nu de CIE is of een ander organisatieonderdeel, al dan niet op legitieme gronden geheimhouding betracht, dit bij andere partijen doorgaans leidt tot negatieve interpretaties omtrent de redenen voor geheimhouding. Dit vormt wel de basis voor een cultuur van onnodige geheimhouding. In essentie kan cultuur onder meer worden beschreven als "*de collectieve constructie van de sociale realiteit*" (Chan 2005: 342). Als volgens de meeste respondenten geheimhouding door een ander immers per definitie suspect en onnodig is, dan is dit de collectieve constructie van de sociale realiteit met betrekking tot geheimhouding. Met andere woorden: er is sprake van een cultuur van onnodige geheimhouding en geheimzinnigheid omdat de meeste medewerkers binnen de politie van mening zijn dat dit het geval is. Of de geheimhouding daadwerkelijk onnodig is, is echter niet goed vast te stellen. Op deze manier is het wel verklaarbaar dat vrijwel alle respondenten van mening zijn dat zij wel aan de eisen van *need to share* voldoen, maar anderen niet.

B: De gevaren van de implementatie van need to share

Ondanks het feit dat veel CIE-ers de uitgangspunten van *need to share* onderschrijven, wijzen zij ook op de mogelijke gevaren van de manier waarop het in de praktijk wordt geïmplementeerd. *Need to share* wordt doorgevoerd door middel van autorisatiemodellen waarbij categorieën politiemedewerkers toegang krijgen tot bepaalde informatie. Tijdens het veldwerk zijn wij herhaaldelijk getuige van discussies over welke medewerkers geautoriseerd zouden moeten worden tot de CIE-informatie. In eerste instantie ging het om de informatie met code 01, maar er werd aangegeven dat uiteindelijk ook 00 en zelfs 200 en 300 informatie met bepaalde afdelingen van de RIO gedeeld moet worden. De autorisatiemodellen zouden daarnaast ook nog worden geautomatiseerd en onderdeel gaan uitmaken van de informatiesystemen waar ook de CIE gebruik van maakt. Dit gaat de CIE-ers vaak veel te ver. Zij onderschrijven het uitgangspunt van 'delen, tenzij…', maar ze geven aan dat in de praktijk het 'tenzij' vaak wordt vergeten of gebagatelliseerd. Volgens respondenten wordt het *need to share* veel te ver doorgevoerd en is er nu meer sprake van een '*free flow of information*', hetgeen niet valt te rijmen met de operationele noodzaak voor geheimhouding. Veel CIE-ers geven dan ook aan dat het delen van informatie steeds meer een doel op zichzelf is geworden, in plaats van een middel tot een doel. Een respondent stelde hieromtrent het volgende.

"*In de breedte ondersteun ik need to share, maar need to share is wel wat anders dan free flow of information en ook anders dan ongebreidelde informatieverstrekking. Er zitten nu eenmaal afbreukrisico's in.*" Interview teamleider CIE (B), februari 2009.

Allereerst bestaat er bij de CIE de angst dat bepaalde informatie mogelijkerwijs te herleiden is naar de bron, hetgeen voor de bron (de informant) levensgevaarlijk kan zijn. Maar CIE-ers wijzen daarnaast op een tweede, volgens hen minstens even belangrijke reden: de zachte informatie die afkomstig is van informanten, is vaak contextgevoelig. Mensen buiten de CIE kennen de specifieke context van de informatie niet, en kunnen – aldus de CIE – deze dan ook niet op waarde schatten en trekken bijgevolg onjuiste (en soms zelfs voor een opsporingsonderzoek gevaarlijke)

conclusies.[265] In de woorden van een leidinggevende van de CIE die het voor de duidelijkheid extra stevig formuleerde: "*Criminele inlichtingen bestaan vaak uit sterke verhalen van hele grote klootzakken, per definitie judassen die je eigenlijk niet goed kunt vertrouwen.*" (Sociaal gesprek hoofd CIE, januari 2009). Je moet dus volgens deze respondent de context van de verhalen kennen om de informatie op waarde te kunnen schatten. Veel tactische collega's kunnen dat volgens de CIE niet.

"*De CIE runt altijd in een wereld van onbetrouwbare figuren (…). Je hebt dus te maken met echt zachte informatie waarvan je niet weet wat je er precies mee kunt. Maar de tactische teams zouden deze informatie graag willen hebben. Het probleem is dat als ik informatie verstrek die niet juist is, ik dit de volgende dag direct om mijn oren krijg. Zo van "waarom laat je ons een hele nacht werken voor niets?" Ze hebben niet door dat tactische informatie ook harde en dus bruikbare informatie is, en CIE informatie zachte en dus moeilijk bruikbaar is. Kijk, onze reputatie gaat natuurlijk naar de knoppen als we informatie gaan verstrekken die niet is veredeld.*" Interview hoofd CIE (A), mei 2007.

De discussie kan volgens ons als volgt worden samengevat. De CIE ziet dat er bij de wijze waarop *need to share* in de praktijk wordt doorgevoerd, geen rekening wordt gehouden met (1) de operationele redenen voor geheimhouding en (2) het belang van de juiste context bij het gebruik van CIE–informatie. Dit zijn de twee grote gevaren van *need to share*, en dit leidt dan ook tot reacties en verzet binnen de CIE.

C: Het verzet tegen need to share

In de discussie hierboven hebben we reeds twee belangrijke reacties waargenomen op het *need to share* streven: (1) informatie wordt niet meer in de informatiesystemen ingevoerd en (2) CIE-en delen onderling minder informatie uit angst dat andere CIE-en teveel informatie delen met 'tactische collega's'.[266] De reactie van een aantal CIE-ers op het van bovenaf opgelegde streven naar *need to share* is dus om sommige informatie niet meer aan het systeem toe te vertrouwen. Immers, als informatie niet in de systemen wordt opgeslagen, kan zij ook niet automatisch worden gedeeld. Sommigen spreken zelfs al van een terugkeer naar de tijd van het notitieboekje. Dit zou betekenen dat het streven naar en afdwingen van meer delen van informatie een averechtse werking heeft: minder informatie in de systemen betekent immers minder informatie om te delen. Dit geldt overigens met name voor het delen van informatie via de formele structuren. Informele informatie-uitwisseling vindt ook plaats via wat wij *old boys networks* noemen. Dit is echter het onderwerp van de volgende subsectie. Wij laten de *old boys networks* in deze subsectie verder buiten beschouwing.

Een andere wijze van ontkomen aan het *need to share* streven is door informatie onder een hogere code te rubriceren dan eigenlijk noodzakelijk is. Wanneer de 01-informatie wordt gedeeld met de RIO's, kan de reactie van CIE-ers zijn om meer informatie weg te schrijven als 00-informatie. En als in de toekomst de 00-informatie meer moet worden gedeeld met anderen die niet tot de CIE behoren, dan zal de reactie zijn om meer informatie de codes 200 of 300 te geven. Deze varianten van wat wij 'de terugkeer van het zakboekje' (of de modernere variant: de

[265] De CIE'ers wijzen met name op dit gevaar wanneer ze het over samenwerking met andere diensten, zoals de AIVD, hebben. Maar ze zien dit toch ook als een reëel gevaar van de interne *need to share*-ontwikkeling. Zie voor de verhouding met de AIVD hoofdstuk acht.
[266] De term 'tactisch' wordt binnen de CIE gebruikt voor niet-CIEers.

stand-alone pc[267]) noemen als primaire persoonlijke databank van de individuele rechercheur is een groot risico voor het slagen van IGP. Het gevolg van 'de terugkeer naar het zakboekje' is dat de informatie versnipperd raakt of wordt verborgen in de systemen. Want zelfs wanneer informatie wel in de systemen ligt opgeslagen, wil dat nog niet zeggen dat de informatie ook daadwerkelijk beschikbaar is: "*Kijk, sommige dingen kunnen wel in systemen staan, maar dat wil nog niet zeggen dat ze toegankelijk zijn.*" (interview recherchekundige RIO, maart 2011). Zo hebben rechercheurs niet zelden informatie in de persoonlijke mappen opgeslagen (de zogenoemde H-schijf), en deze mappen worden niet gedeeld met andere collega's. Voor de CIE en de informatieafdelingen is deze informatie zeer moeilijk tot niet te bereiken, dit tot frustratie van de medewerkers.

"*Collega's zetten informatie op de H-schijf, dat is de eigen schijf waarop ik bijvoorbeeld alleen maar mijn reiskosten-declaratie heb staan. Maar sommige collega's hebben daar om één of andere vreemde reden operationele info op staan. (…) In plaats van dat je beseft dat je voor een groter geheel bezig bent, ga je je eigen product, dat een onderdeel is van een grotere opdracht wegzetten zonder dat iemand anders er dan bij kan. En dan vasthouden alsof het jouw informatie is, terwijl het helemaal niet jouw informatie is: jij gaat met informatie van anderen aan het werk, maakt daar een product van ten behoeve van advisering, aan de sturing van de opsporing. En dan vind ik het onbegrijpelijk dat zo iemand dit op deze manier weg zet, zo dat niemand erbij kan.*" Interview recherchekundige RIO (A), mei 2009.

Voorts wijzen respondenten ons op het risico dat een te brede autorisatie voor CIE-gegevens leidt tot problemen met andere CIE-en. Immers, als deze CIE-en bemerken dat een andere CIE te veel informatie deelt, dan is de kans dat daar informatie van andere CIE-en bij zit aanzienlijk. Dit heeft te maken met de systemen waarin de informatie wordt opgeslagen. Met een brede autorisatie is het mogelijk om deze gegevens te zien. Dit maakt regionale CIE-en huiverig om informatie te delen en is uiteindelijk funest voor het onderlinge vertrouwen. Een respondent wees ons op het belang van de afscherming en de gevolgen voor de binnen de CIE geldende waarden.

"*Het allergrootste goed binnen de cie is bronbescherming. Daarnaast wil je de beste producten maken, maar het gaat met name om bronbescherming. Het is dan ook een hele kleine wereld waarin iedereen iedereen kent. Daarom hebben we binnen de CIE een aantal gouden regels: je hebt intern weinig geheimen voor elkaar, je helpt elkaar, vertrouwt elkaar en bent betrouwbaar. Dat moet ook wel. Bronbescherming is het allerbelangrijkste, en als daar iets in dreigt mis te gaan, dan valt de bodem onder de CIE weg. Veranderingen in processen die gevolgen kunnen hebben voor de afscherming blijven dan ook niet onopgemerkt. Als de hoogste leiding bepaalde autorisaties geeft voor CIE-informatie en mensen zonder CIE-status, dan hangt er direct een collega aan de lijn en die vraagt je direct 'klopt dit of dat?' En als het klopt, dan zijn ze bang voor de afscherming en verstrekken ze niks meer.*" Interview analist CIE (G), maart 2011

Medewerkers van de CIE gaven tijdens interviews aan dat het al is voorgekomen dat het uitwisselen van CIE-gegevens tussen sommige CIE-en is opgeschort vanwege

[267] Een *stand-alone* pc is een computer die niet op een netwerk is aangesloten. Deze maken dan ook geen gebruik van de standaard ICT-voorzieningen die de *need to share*-gedachte moeten stimuleren.

deze reden. Overigens tekenen wij hierbij aan dat het niet gaat om identificerende gegevens (dus gegevens die de identiteit van de informant weggeven). Deze gegevens blijven te allen tijden afgeschermd voor andere CIE-en. En zelfs binnen een CIE zijn slechts de runners en het (plaatsvervangend) hoofd CIE op de hoogte van de identiteit van de informant. Het risico van de 00 en 200 informatie is dat deze gecombineerd met andere informatie mogelijk een indicatie opleveren van de identiteit van de informant. Hier dient terughoudend mee om te worden gegaan. Een neveneffect van het doorvoeren van *need to share* is dus dat informatie juist niet meer wordt gedeeld. CIE-ers wijzen er ook op dat informanten met de CIE praten omdat ze erop kunnen vertrouwen dat hun identiteit wordt afgeschermd. Indien teveel CIE-informatie wordt gedeeld met buitenstaanders is dit niet meer te garanderen, met als gevolg dat het bestaande en potentiële nieuwe informanten zal afschrikken.

De twee hierboven beschreven reacties van de CIE op het *need to share* streven binnen de Nederlandse politie zijn de belangrijkste vormen van verzet tegen dit streven. *Need to share* binnen de CIE leidt dan ook in zekere zin tot een paradox: hoe meer de nadruk wordt gelegd op het delen van informatie, des te minder informatie door CIE-ers zal worden gedeeld. Veranderingen in organisaties kunnen echter altijd rekenen op een zekere mate van verzet van de werkvloer. Het verzet tegen verandering is niet per definitie succesvol. Bij de politie lijkt dit volgens onze respondenten echter wel het geval te zijn: van *need to share* komt volgens hen in de praktijk te weinig terecht. Wij sluiten deze subsectie af met een antwoord op de vraag hoe het komt dat *need to share* in de politiepraktijk niet goed kan worden ingevoerd.

D: Problemen bij de implementatie van need to share

In subsectie 2.3.2 hebben wij drie benaderingen van geheimhouding beschreven die ook gelden voor de CIE (en in mindere mate de RIO's). Wij maakten daar een onderscheid in (1) de institutionele benadering, (2) de sociale benadering en (3) de operationele benadering. Voor een succesvolle implementatie van *need to share* is het van belang dat deze benaderingen van geheimhouding worden beïnvloed en deels worden weggenomen met als uiteindelijke doel de geheimhouding tot een noodzakelijke minimum te beperken. Wij laten de operationele benadering grotendeels buiten beschouwing, omdat deze benadering onveranderlijk is: zij zal altijd een rol spelen en het is onwaarschijnlijk dat de aan deze benadering ten grondslag liggende redenen voor geheimhouding zullen worden weggenomen. Wij stellen echter vast dat zowel de institutionele als de sociale benadering door *need to share* niet wordt weggenomen, terwijl de redenen die uit deze benaderingen voortvloeien leiden tot de niet-gerechtvaardigde geheimhouding waaraan *need to share* een einde probeert te maken.

Het NIM lijkt uit te gaan van twee oplossingen voor het probleem van de ongerechtvaardigde geheimhouding: (1) een juridische oplossing, waarbij nieuwe wet- en regelgeving dient te leiden tot minder juridische barrières, en (2) een ICT-oplossing, waarbij verbeterde informatiesystemen moeten leiden tot meer geautomatiseerde informatie-uitwisseling. Kennelijk bestaat er binnen de politie dus het beeld dat informatie niet wordt gedeeld omdat er juridische en technologische barrières zijn. Dit is echter slechts een deel van de verklaring voor het bestaan van geheimhouding. De andere belangrijke redenen voor geheimhouding die een onderdeel vormen van de institutionele benadering zijn (1) het *free-rider* probleem, waarbij anderen de gedeelde informatie gebruiken voor eigen successen, (2) het concurrentieprobleem, waarbij het delen van informatie de autonomie van de eigen

organisatie aantast en (3) het cultuurprobleem, waarbij het delen van informatie als een te groot risico wordt gezien (zie subsectie 2.3.2). In het NIM wordt bij de beschrijving van *need to share* echter met geen van deze drie problemen rekening gehouden. Sterker nog, in bepaalde opzichten worden de problemen juist versterkt. Dit geldt met name voor het *free-rider* probleem en het concurrentieprobleem. Wij zullen beide problemen hieronder kort uitwerken voor de Nederlandse situatie van IGP en het NIM.

Met de oprichting van de RIO-structuur is er een extra afdeling opgericht die een essentiële rol dient te vervullen met betrekking tot het informatieproces. In veel korpsen hebben de RIO's formeel een belangrijke taak bij het adviseren van stuurgroepen over te nemen strategische, tactische en operationele beslissingen. Voorheen hadden de CIE-en en de tactische teams hierin een veel grotere rol. Deze rol is met de komst van de RIO in theorie gemarginaliseerd. De RIO's beschikken echter niet over eigen informatie, maar zijn afhankelijk van de informatievoorziening door de CIE en de tactische teams. Een veelgehoorde klacht binnen de CIE is dat zij (de CIE) beschikt over de kennis en kunde (en de informatie) om daadwerkelijk goed advies te geven, maar dat de RIO's dit nu doen. De RIO's hebben aldus veel invloed, maar missen de kennis en kunde die de CIE wel heeft en dat leidt tot slechte besluitvorming, aldus medewerkers van de CIE. Binnen de CIE bestaat er dan ook erg veel weerstand tegen het delen van informatie met de RIO's. In de praktijk verstrekken de CIE-en daarom bijzonder weinig aan de RIO's: de primaire afnemer van processen-verbaal zijn nog steeds de tactische onderzoeksteams. In sommige korpsen is onder andere vanwege de concurrentie tussen de CIE en de RIO's besloten om de CIE onderdeel te maken van de RIO. Dit is echter een schijnoplossing, omdat de CIE juridisch en organisatorisch gezien nog steeds een *status aparte* heeft. Er is immers geen ander organisatieonderdeel die informanten mag runnen, en de operationele noodzaak voor geheimhouding blijft bestaan, waardoor de fysieke afscherming van de CIE ook nog steeds noodzakelijk is. Met andere woorden: met het veranderen van het organogram is de effectieve organisatie nog niet veranderd.

De derde reden voor geheimhouding (het cultuurprobleem) is ook niet opgelost. Het risico van het delen van CIE-informatie is ongewijzigd: de baten wegen niet op tegen de kosten. Dit risico hebben we hierboven reeds beschreven. Indien veel informatie wordt gedeeld met de RIO, schorten andere CIE-en de onderlinge informatie-uitwisseling op. Relevante informatie en inzichten worden zo gemist en de desbetreffende CIE raakt geïsoleerd. Wij noemen hiernaast nog twee risico's van het delen van informatie. Het tweede risico betreft de kerntaak van de CIE: het runnen van informanten. Indien de CIE teveel informatie deelt met anderen, kan dit tot gevolg hebben dat informanten niet meer met de CIE durven te praten uit angst dat hun identiteit te snel bij teveel mensen bekend raakt. Op deze manier droogt de informatie-positie van de CIE op, hetgeen door veel CIE-ers als een groot risico wordt gezien. Het derde risico is een persoonlijk risico voor de individuele CIE-er die teveel informatie deelt. De sanctie op het delen van 00, 200 en 300-informatie met mensen buiten de CIE wordt door een CIE-er als volgt benoemd: "*je vliegt eruit. En als dat niet gebeurt, dragen je collega's je het nog wel een tijdje na. Bij twijfel niet inhalen dus.*" (CIE-runner, sociaal gesprek, januari 2010). Van individuele CIE-ers kan dus ook niet worden verwacht dat ze snel informatie delen: de persoonlijke risico's zijn te groot.

Met betrekking tot de sociale redenen voor geheimhouding merken wij op dat de cultuur van de onnodige geheimhouding waar het NIM en *need to share* zich op richten uit een collectieve sociale constructie voortkomt. Het is een gedeelde

opvatting dat er onnodige geheimhouding wordt betracht. Zolang er geheimhouding bestaat, zal in de collectieve sociale constructie uitgegaan worden van *onnodige* geheimhouding. Dit komt door de aard van geheimhouding. In de perceptie van degenen die niet tot de dragers van geheim behoren, is geheimhouding al snel onnodig. Zij zullen zichzelf immers snel betrouwbaar achten. En een dergelijke collectieve sociale constructie laat zich niet gemakkelijk wijzigen door juridische en technologische veranderingen. Met betrekking tot de cultuur van geheimhouding is dan ook sprake van een paradox. De cultuur van geheimhouding is niet tastbaar: het is een idee, een gevoel 'dat er meer speelt dan men mag weten'. Dit gevoel zal onzes inziens blijven bestaan zolang geheimhouding bestaat. De cultuur van onnodige geheimhouding waarop het NIM en *need to share* zich richten, staat dan ook los van de *daadwerkelijke* geheimhouding. Het zou verstandiger zijn als *need to share* zich zou richten op het wegnemen van de institutionele redenen van geheimhouding.

7.6.2 Doelstelling 2: *old boys networks*

Netwerken zijn, evenals markten en bureaucratieën, een vorm van sociale organisatie (Thompson et al. 1998). Een netwerk bestaat uit "*(in)formele relaties tussen in essentie gelijke sociale actoren*" (Gill en Phythian 2006: 39). Wij maken een onderscheid tussen formele en informele netwerken. Formele netwerken gaan voor de informatie-uitwisseling met name uit van ICT-systemen en zij zijn daarmee geïnstitutionaliseerd. Daarnaast zijn deze formele netwerken in belangrijke mate gereguleerd: de WPG bepaalt welke informatie met wie mag worden gedeeld, de Politiewet bepaalt (onder meer) wie er kan worden gerekend tot het formele politienetwerk en het Wetboek van Strafvordering bepaalt onder meer aan wie er toestemming gevraagd moet worden voor het verkrijgen van informatie. Een politieorganisatie die volgens IGP wil werken doet er in theorie goed aan om haar informatie- en communicatienetwerk te institutionaliseren. Anders loopt zij het risico dat belangrijke informatie verloren gaat, of in de organisatie verdwijnt en niet toegankelijk is (zie Van Calster et al. 2010: 178). De Nederlandse politieorganisatie en het NIM gaan met betrekking tot IGP dan ook met name uit van formele, geïnstitutionaliseerde communicatie en netwerken.

Binnen de politieorganisatie bestaan ook informele netwerken die zijn gebaseerd op onderling vertrouwen. Deze informele netwerken vormen een alternatief voor de formele netwerken. Via de informele relaties wordt informatie uitgewisseld. Deze netwerken bestaan met name bij de gratie van vertrouwen tussen de actoren (zij vormen de noden, de knooppunten in het netwerk): het zijn sociale netwerken. In tegenstelling tot de formele netwerken zijn informele netwerken doorgaans flexibel, en dat is dan ook een belangrijke verklaring voor het bestaan van informele sociale netwerken.

"(…) *Daar drijft de recherche op, volgens mij. Veel meer dan op systemen. Systemen zijn meer een soort geheugen, het werkgeheugen zeg maar, het korte termijn geheugen zit gewoon in de mensen zelf.*" Interview recherchekundige (B), maart 2011.

Wij noemen deze netwerken *old boys networks*. De term *old boys networks* is echter niet onproblematisch. Wij behandelen twee problemen. Allereerst heeft de term doorgaans een negatieve connotatie en roept al snel een beeld op van nepotisme. Via een *old boys network* worden bijvoorbeeld baantjes vergeven aan leden van het netwerk en worden buitenstaanders geweerd van bepaalde posities. Dit is niet het type

old boys network waar wij op doelen: het gaat ons om de informele wijze van informatie-uitwisseling. Zaken als nepotisme laten wij in dit onderzoek buiten beschouwing. Een tweede probleem is het formuleren van een definitie van een *old boys network*. Dit maakt het onderzoeken van het fenomeen erg lastig. Want wanneer is er sprake van een *old boys network*? Collega's die een keer met elkaar bellen, vormen nog niet onmiddellijk een *old boys network*. Om van een *old boys network* te kunnen spreken, is een zekere mate van bestendigheid van het netwerk vereist. Het is echter ook een informeel netwerk en veranderlijk. Dit maakt het moeilijk om bijvoorbeeld het bestaan en de werking van specifieke, concrete netwerken aan te tonen. Dit probleem speelt nauwelijks bij ons onderzoek. Wij zijn in het kader van onze probleemstelling en de onderzoeksvragen met name geïnteresseerd in de vraag of dergelijke netwerken in het algemeen bestaan en in hoeverre deze netwerken conflicteren met de formele netwerken voor wat de informatie-uitwisseling betreft. Welke netwerken er precies bestaan en wie daartoe behoren is in het kader van ons onderzoek aldus niet relevant.

Tijdens ons onderzoek hebben wij het bestaan van informele communicatienetwerken kunnen waarnemen. Veelal nemen politiemensen eerst informeel contact op met bekenden elders in het korps of in het land en bewandelen zij later de formele weg. Ons onderzoek bracht naar voren dat deze informele netwerken veelal het gevolg zijn van barrières in het formele communicatiesysteem. Politiemensen zoeken in de praktijk naar manieren om deze barrières te omzeilen en een informele communicatie is één van die manieren. Deze barrières leiden tot wantrouwen bij de politiemensen ten opzichte van het invoeren van informatie in de computersystemen. Uit onze observaties blijkt dat dit wantrouwen onder andere tot gevolg heeft dat politiemensen kiezen voor het directe contact met collega's die zij vertrouwen. Het komt ons voor dat de anonimiteit van het computersysteem en de geautomatiseerde informatiedoorstroming een negatieve impact hebben op de bereidheid bij bepaalde politiemensen om informatie aan het computersysteem toe te vertrouwen. Het hangt af van de specifieke medewerker hoe ver dit gaat, maar het hiervoor genoemde wantrouwen in het computersysteem heeft volgens enkele respondenten mogelijk negatieve effecten op het doorvoeren van het *need to share*-principe. Het gegeven dat veel politiemensen in toenemende mate gebruik maken van een zakboekje, waarin zij informatie opnemen die zij niet aan het computersysteem overdragen, draagt er toe bij dat een *old boys network* kan ontstaan of blijven bestaan. Deze informele communicatie staat in het politiejargon overigens bekend als de politie-politie-methode.

Wij hebben meerdere oorzaken voor de populariteit van de politie-politie-methode waargenomen, die allemaal dezelfde gemene deler lijken te hebben: tijdsbesparing. Via de informele weg van de politie-politie-methode wordt veel sneller informatie verkregen dan via de formele weg. Wij constateerden drie situaties waarin de politie-politie-methode beduidend sneller werkt dan de formele wijze van informatie-uitwisseling. Situatie 1: informatie zou in de systemen (BVO *et cetera*) moeten zitten, maar is niet snel te vinden. Situatie 2: medewerkers worden overspoeld met informatie (*data-overload*) en kunnen niet tijdig bepalen met welke informatie ze het beste kunnen werken. Situatie 3: de medewerker heeft bepaalde informatie of aannames waarvan hij op korte termijn de validiteit moet vaststellen. Wij zullen elke situatie kort behandelen.

Situatie 1: onvindbare informatie

Onze respondenten gaven aan dat een belangrijke reden voor het gebruik van de informele weg voor het opvragen van informatie ligt in het feit dat niet alle informatie terug te vinden is in de computersystemen. De meeste respondenten merkten op dat er nogal wat aan het formele systeem schort. Een grote klacht is dat het werken met het systeem nogal omslachtig en bewerkelijk is (zie De Koning 2010; zie ook subsectie 7.4.1). Het systeem is een grote bron van ergernis voor zowel de runners als de analisten, omdat zij zelf op zoek moeten gaan naar relaties tussen informatie en deze zelf in het systeem moeten aanbrengen. Het zoeken op een specifieke naam levert zelden alle relevante informatie op: veel informatie is onder andere (onjuiste) codes weggeschreven en als zodanig niet toegankelijk voor runners. Daarnaast wordt bepaalde informatie ook eenvoudigweg niet in de systemen opgenomen (zie subsectie 7.6.1). In veel gevallen loont het om dan maar direct met de rechercheur of een teamleider contact op te nemen. Uit de observaties en de interviews bleek dat dit veelvuldig gebeurde: runners en analisten namen telefonisch contact op of kwamen bij elkaar over de vloer en wisselden buiten de formele kanalen informatie uit.

Situatie 2: data overload

Een ander probleem dat we in de praktijk zijn tegengekomen, is dat van de *data-overload* (zie Sheptycki 2004; zie ook sectie 2.2). Grootschalige onderzoeken leveren vaak ongelooflijke hoeveelheden data op, veel meer dan de gemiddelde analist of rechercheur kan verwerken. Naast de grote hoeveelheden informatie uit telefoontaps en observaties worden er tegenwoordig ook veel computers in beslag genomen en wordt andere digitale informatie verzameld, hetgeen alleen maar meer data oplevert. Tel daarbij de informatie op uit open bronnen, en de te verwerken hoeveelheid informatie is enorm. Het loont ook in deze gevallen om direct contact te hebben met een collega in plaats van zelf in de systemen op zoek te gaan naar informatie. Zij kunnen doorgaans aangeven welke informatie van belang is en kan zijn en dit levert aanzienlijke tijdswinst op dan zelfstandig op zoek gaan. Overigens bleek tijdens ons onderzoek dat politiemedewerkers ook contact met collega's om ze tijdig te waarschuwen dat bepaalde informatie bijvoorbeeld na een informanten-gesprek binnen is gekomen. Deze informatie is dan nog niet verwerkt, maar via de informele kanalen krijgt iemand wel tijdig een waarschuwing. In deze gevallen werken de formele communicatielijnen vaak langzaam en dus vertragend. Juist omdat opsporingsonderzoeken vaak een zekere tijdsdruk kennen, is het dikwijls niet wenselijk om te wachten totdat bepaalde informatie in het systeem wordt ingevoerd. Het zijn precies deze geïnstitutionaliseerde en structurele problemen die ervoor zorgen dat politiemensen vaak overgaan tot informele weg om informatie te verkrijgen.

Situatie 3: valideren informatie en aannames

Vaak beschikken medewerkers van de CIE en van de RIO over onvoldoende informatie om bepaalde vermoedens en aannames (hypotheses) te verifiëren of falsificeren. Daarnaast komt het voor dat de betrouwbaarheid en waarde van de informatie moeten worden ingeschat. In deze gevallen is daar extra informatie voor nodig. De politie-politie-methode wordt vaak gebruikt om deze aanvullende informatie te verkrijgen. Officieel dienen dergelijke verzoeken via een

geïnstitutionaliseerde, formele informatiestroom te lopen. Met de politie-politie-methode en de informele netwerken wordt deze route omzeild. Wanneer bepaalde informatie aanwezig is en beschikbaar kan worden gesteld, gaat men er alvast mee aan de slag, terwijl intussen de formele kanalen worden gebruikt om alsnog op een formeel juiste manier aan de informatie te komen. Wij hebben echter ook vernomen dat in bepaalde gevallen het formele traject helemaal wordt overgeslagen. Dit gebeurt met name bij het falsificeren van bepaalde vermoedens en aannames: bij falsificatie wordt het vermoeden of de aanname niet meer gebruikt, en het wordt gezien als tijdsverspilling om de achterliggende informatie alsnog (rechtmatig) te verkrijgen. Deze gefalsificeerde aannames en vermoedens zullen immers niet worden gebruikt in de onderzoeken en spelen geen rol van betekenis meer in het opsporings- of inlichtingenproces.

7.6.3 Tussenconclusies

Met betrekking tot het verstrekken van informatie hebben wij de volgende tussenconclusies, ook hier praktijkbevindingen genoemd.

Praktijkbevinding 6a: De uitgangspunten van *need to share* worden binnen de CIE geaccepteerd en onderschreven. Desondanks is er volgens de binnen de politie heersende collectieve perceptie met betrekking tot de CIE sprake van een cultuur van onterechte geheimhouding.

Praktijkbevinding 6b: Het delen van informatie is bij *need to share* een doel op zichzelf geworden. Het delen van teveel informatie kan in strijd zijn met de operationele redenen voor geheimhouding en betekent dat informatie uit de context wordt gehaald.

Praktijkbevinding 6c: De implementatie van *need to share* leidt binnen de CIE tot twee vormen van verzet: (1) informatie wordt niet meer in de informatiesystemen ingevoerd en (2) CIE-en wisselen onderling geen informatie meer uit. Het gevolg is mogelijk dat de algemene informatiepositie van de CIE slechter wordt.

Praktijkbevinding 6d: Omdat *need to share* zich niet richt op het wegnemen van de institutionele en sociale redenen voor geheimhouding, is de implementatie vooralsnog niet succesvol.

Praktijkbevinding 6e: De formele informatie- en communicatienetwerken van de politie kennen belangrijke tekortkomingen. Zo is informatie onvindbaar, is er sprake van data-overload en is de formele communicatie bewerkelijk en tijdrovend. Om hieraan te ontkomen bestaan er binnen de Nederlandse politie (en de CIE) informele communicatienetwerken: varianten van het *old boys network*.

Concluderend

Op basis van de bovenstaande praktijkbevindingen komen we tot de volgende conclusie. Het belang van het delen van informatie wordt ook binnen de CIE onderschreven. Het gevaar is echter dat *need to share* steeds meer een doel op zichzelf wordt, in plaats van een middel om het politiewerk te verbeteren en tot een succesvolle implementatie van IGP te komen. De twee doelstellingen van *need to*

share, te weten het doorbreken van de onnodige geheimhouding en het formaliseren van de informele informatie-uitwisseling en communicatie zijn (nog) niet behaald. Wellicht dat dit wel gelukt als de belangrijkste redenen voor geheimhouding worden weggenomen. Slechts als het NIM oplossingen biedt voor de problemen uit de beschreven drie situaties van (1) onvindbare informatie, (2) informatie-overload en (3) valideren informatie en aannames, kunnen de informele informatie-infrastructuren (de *old boys networks*) worden doorbroken. Vooralsnog hebben deze infrastructuren nog steeds een grote meerwaarde voor de informatie-uitwisseling in de dagelijkse politiepraktijk, en dit zal de komende jaren nog wel zo blijven.

7.7 Hoofdstukconclusie en antwoord op OV 3

In dit hoofdstuk hebben wij de praktijk van IGP bij de CIE en de RIO beschreven. Aan de hand van praktijkbevindingen hebben wij geprobeerd vast te stellen in hoeverre IGP is geïmplementeerd in de Nederlandse CIE-praktijk (OV 3). Wij hebben allereerst (1) de vraag beantwoord in hoeverre de medewerkers bekend zijn met IGP. Vervolgens hebben wij achtereenvolgens de volgende elementen van IGP behandeld: (2) de sturing van de CIE, (3) de verzameling van informatie, (4) de verwerking van informatie, (5) de analyse van informatie en (6) de verstrekking van informatie. Voor vrijwel alle elementen komen wij tot de conclusie dat er in de praktijk weinig van terechtkomt. Er is nauwelijks sprake van sturing, de informatieverzameling is grotendeels reactief en de informatieverwerking wordt bemoeilijkt door falende informatiesystemen en tekortschietende informatieprocessen.

Criminaliteitsanalyse wordt deels gebruikt bij de besluitvorming, maar vooral in die gevallen waarbij de analist ruimte overlaat aan de leidinggevenden voor de interpretatie. Hierom wordt met name de strategische analyse nauwelijks gebruikt bij de effectieve besluitvorming, terwijl het juist deze vorm van op de toekomst gerichte analyse is die zou moeten kunnen leiden tot een daadwerkelijke intelligence-benadering. Alhoewel het *need to share*-streven door veel medewerkers op hoofdlijnen wordt onderschreven, wordt het in de praktijk zo ver doorgevoerd dat het tot verzet binnen de CIE leidt: informatie wordt niet meer in de systemen ingevoerd en CIE-en wisselen onderling minder informatie uit. Het resultaat is uiteindelijk voor de totale informatiepositie van de CIE (en de RIO) nadelig. Wij moeten dan ook met betrekking tot *need to share* concluderen dat de doelstellingen ervan niet worden behaald. De cultuur van onnodige geheimhouding blijft bestaan omdat dit inherent is aan geheimhouding en er aan de onderliggende redenen voor geheimhouding niets wordt gedaan. Het antwoord op OV3 is dat de CIE nogweinig volgens IGP werkt.

Hieronder proberen wij de bevindingen en het antwoord op OV3 naar een hoger abstractieniveau te brengen door de drie belangrijkste overkoepelende redenen te benoemen die onzes inziens aan de falende implementatie van IGP ten grondslag ligt. Het gaat dan om (1) onduidelijkheid omtrent IGP en wat het concept beoogt te bereiken, (2) hardnekkige structuurkenmerken van de politie die implementatie van elementen van IGP bemoeilijken en (3) de weerbarstige politiecultuur die zich moeilijk laat veranderen.

Ad (1) Onduidelijkheid omtrent IGP en diens doelstellingen

Eén van de essentiële voorwaarden voor het succesvol doorvoeren van veranderingen is dat er duidelijkheid is omtrent wat met de verandering wordt beoogd en waarom de veranderingen worden doorgevoerd. Dit laat onverlet dat een zekere ambiguïteit met

betrekking tot IGP in bepaalde gevallen voordelig zou kunnen zijn. IGP wordt voorgesteld als een fundamentele verandering: IGP zou zelfs een paradigmaverandering behelzen. Dit zou betekenen dat juist voor IGP geldt dat er duidelijkheid nodig is omtrent het concept. In de praktijk blijkt dit echter duidelijk niet het geval te zijn. Het label 'IGP' wordt op zoveel verschillende ontwikkelingen geplakt, dat het een onderscheidend vermogen ten opzichte van andere concepten verliest. Dit bemoeilijkt de implementatie van het concept aanzienlijk, want de vraag is wat er precies wordt geïmplementeerd. Het gebrek aan duidelijkheid omtrent inhoud, nut en noodzaak van IGP zal volgens de inzichten van het veranderingsmanagement de implementatie ervan bemoeilijken. De onduidelijkheid omtrent IGP komt deels voort uit onbekendheid met de complexiteit van interne processen en de interne dynamiek binnen de politieorganisatie in het algemeen. Zo wordt er uitgegaan van het bestaan van een *need to know* cultuur zonder dat is geanalyseerd wat dit precies betekent en waarom deze cultuur bestaat. Vanwege de zeer beperkte benadering van geheimhouding wordt er gekozen voor een zeer beperkte oplossing voor het (vermeende) probleem: een juridisch en ICT-matig autorisatiemodel moet de geheimhouding tegengaan. Maar de institutionele, sociale en operationele redenen voor geheimhouding blijven grotendeels ongewijzigd. Het mogelijke gevolg is meer en hardnekkige geheimhouding en een versterkte interne concurrentie tussen de eenheden. En dit is juist wat IGP probeert te voorkomen. Het was verstandig geweest als de 'eerst denken en dan doen' benadering die IGP voorstaat ook bij de ontwikkeling en implementatie van het concept was gevolgd. Men is te snel uitgegaan van ingewikkelde procesmodellen maar is daarbij voorbij gegaan aan de realiteit van het politiewerk. Dit brengt ons tot de volgende verklaring: de hardnekkige structuurkenmerken van de politie.

Ad (2) De hardnekkige structuurproblemen van de politie

Sommige structuurproblemen zijn van tevoren weliswaar voorzien, maar blijken te hardnekkig en complex om met IGP te worden opgelost. Ze vormen echter wel een belangrijke barrière tegen de implementatie van IGP. Voordat IGP succesvol kan worden geïmplementeerd, zullen de belangrijkste structuurproblemen moeten worden opgelost. Structuurproblemen zijn echter zeer moeilijk op te lossen. Het woord 'structuur' zegt het immers al: ze zijn verbonden met wijze waarop de organisatie is ingericht en vormgegeven. Wij zien een structuurprobleem dan ook als een probleem dat voortkomt uit de inrichting en vormgeving van de organisatie. Het oplossen van structuurproblemen vereist een aanpassing van de inrichting en vormgeving van de organisatie, en dit vergt grote inspanningen en een lange-termijn-planning. Voor een 'paradigmawijziging' als IGP is dit echter noodzakelijk. Maar over welke structuurkenmerken hebben wij het?

Met name de ICT-systemen bij de politie vormen een dergelijk hardnekkig structuurprobleem. De ICT-systemen zijn gebruikersonvriendelijk en er verdwijnt veel informatie in het systeem. Een versnipperde informatiepositie is het gevolg. Omdat IGP met name uitgaat van de productbenadering van intelligence, waarbij data aan de basis ligt van de informatie- en intelligenceproducten, werken systeemproblemen als die met de ICT verlammend voor de implementatie van het gehele concept. Een ander structuurelement is de feitelijke hiërarchie van de politieorganisatie. Daar waar de politie formeel een hiërarchische organisatie is met een duidelijk rangen-systeem, blijkt er in de praktijk met name sprake te zijn van een grote discretionaire ruimte voor de politieman op straat. Dit volgt uit de aard van het

politiewerk: de meeste werkzaamheden van de lagere politiemedewerkers vinden buiten het bereik van de leidinggevenden plaats, waardoor effectieve sturing eigenlijk niet mogelijk is. Met IGP wordt geprobeerd om *top-down* veranderingen door te voeren zonder dat er rekening wordt gehouden met de feitelijke structuur van de organisatie. Dergelijke sturing vanuit de hiërarchie is bij een *street-level bureaucracy* zoals de politie vrijwel onmogelijk. Het derde en laatste structuurkenmerk dat wij benoemen is de onderlinge concurrentie tussen de afdelingen. De politie is een bureaucratische organisatie met veel interne subculturen. Tussen bureaucratische organisaties en bureaucratische subculturen is vaak sprake van concurrentie. Met de oprichting van de RIO is er een organisatieonderdeel in het leven geroepen die een deel van de CIE-taak moet vervullen. Dit leidt tot verregaande onderlinge concurrentie. De CIE kan met name macht uitoefenen door weinig informatie aan de RIO te verstrekken. Dit is echter in strijd met het gedachtegoed van IGP en *need to share*. De concurrentie tussen de verschillende organisatieonderdelen moet worden opgelost voordat een succesvolle implementatie van IGP mogelijk is.

IGP heeft vooralsnog geen antwoord op deze structuurproblemen. Dit is ook niet verwonderlijk: het zijn problemen die verweven zijn met de politiestructuur en die worden niet gemakkelijk opgelost. Desalniettemin vormen het belangrijke barrières tegen de implementatie van IGP.

Ad (3) De weerbarstige en ongrijpbare politiecultuur

De laatste barrière tegen een succesvolle implementatie van IGP is de weerbarstige politiecultuur. Evenals structuurproblemen die moeilijk op te lossen zijn, is de politiecultuur moeilijk te veranderen. Dit komt omdat een cultuur ongrijpbaar is. Wij hebben cultuur in subsectie 7.6.1 gedefinieerd als "*de collectieve constructie van de sociale realiteit*". Dit bestaat uit de manier waarop politiemensen naar de wereld kijken en hoe ze zich vervolgens in de wereld manifesteren. Wij hebben een aantal cultuurelementen gezien die een mogelijke barrière vormen tegen het implementeren van IGP bij de CIE en de RIO.

Allereerst zijn medewerkers van de CIE en in mindere mate de RIO wars van innovaties, of dit nu technologische innovaties of innovaties van het werkproces betreft. Ze zijn doorgaans conservatief en niet snel geneigd om mee te gaan in veranderingen. Voor een paradigmawijziging zoals IGP is dit een behoorlijke barrière: het belemmert de acceptatie van nieuwe ideeën en werkwijzen. Een tweede cultuurelement is de waan-van-de-dag-mentaliteit. Veel politiemedewerkers zijn gevormd door het traditionele, reactieve politiewerk en laten zich hierdoor (bewust of onbewust) leiden bij het nemen van beslissingen. Deze mentaliteit zorgt er bijvoorbeeld voor dat strategische lange-termijn-beslissingen niet worden genomen en dat er van proactiviteit nauwelijks sprake is. Dit zijn beide essentiële kenmerken van IGP. Het derde en laatste cultuurkenmerk dat wij hier zullen noemen, is de *need to know*-cultuur. Binnen de CIE is er sprake van een verregaande geheimhouding en dit zorgt ongetwijfeld voor een cultuur van geheimhouding. Van een cultuur van ongerechtvaardigde geheimhouding lijkt in zekere zin sprake te zijn. De collectieve constructie van de sociale realiteit met betrekking tot anderen die geheimhouding betrachten gaat namelijk uit van het beeld dat er tot op zekere hoogte sprake is van ongerechtvaardigde geheimhouding. Dit laat onverlet of de geheimhouding in werkelijkheid ongerechtvaardigd is: het enkele bestaan van geheimhouding doet anderen reeds vermoeden dat deze geheimhouding in ieder geval deels ongerechtvaardigd is. Dit laat duidelijk zien wat het probleem van cultuur is: het gaat

om een perceptie van de werkelijkheid, en dergelijke percepties zijn erg moeilijk te beïnvloeden. Dit maakt de politiecultuur erg weerbarstig.

De drie door ons geformuleerde redenen waarom IGP nog niet is geïmplementeerd, vormen barrières tegen IGP die afgebroken dienen te worden voordat er van IGP gesproken kan worden. Dat dit niet gemakkelijk is, zal duidelijk zijn. Dit stemt wellicht pessimistisch met betrekking tot IGP in de praktijk en de politieorganisatie in het algemeen. Alhoewel veel problemen inderdaad ernstig zijn, willen wij hier ook een nuancering aanbrengen. Wij hebben de CIE en de RIO bekeken aan de hand van de uitgangspunten van IGP. We hebben het al vaker gesteld: IGP behelst een paradigmawijziging. Feitelijk heeft IGP dan ook tot doel om tot een geheel nieuwe politieorganisatie te komen. Dat deze doelstelling niet gemakkelijk kan worden bereikt, is niet meer dan logisch. Wanneer de CIE en de RIO vanuit een ander, meer traditioneel perspectief worden bekeken, dan zullen de conclusies wellicht heel anders (positiever) luiden.

8| De AIVD en de CIE: een moeizame relatie

In dit hoofdstuk behandelen wij OV4: *Wat is de verhouding tussen de AIVD en de CIE in de praktijk?* Daartoe geven we allereerst kort een overzicht van de traditionele conceptuele verhouding tussen de diensten (sectie 8.1). Wij noemen dit een conceptuele verhouding omdat het ziet op algemene, abstracte kenmerken van de beide diensten. Daarna schetsen wij de veranderingen die in deze conceptuele verhouding zijn opgetreden en de gevolgen van deze veranderingen voor de verhouding tussen de diensten in de praktijk (sectie 8.2). Deze veranderingen in combinatie met de belangen die zijn gemoeid met de bestrijding van terrorisme maken afstemming en samenwerking tussen de AIVD en de intelligence-organisatie van de politie (de CIE/RIO[268]) noodzakelijk. Een essentiële voorwaarde hiervoor is onderling vertrouwen. In welke mate er vandaag de dag (2012) sprake is van vertrouwen en wat vertrouwen precies inhoudt, is het onderwerp van de sectie 8.3. In de hierop volgende secties behandelen wij de drie elementen van vertrouwen zoals beschreven in de theorie van Hardin (2005), te weten de driehoeksrelatie (sectie 8.4), de reden voor vertrouwen (sectie 8.5) en het risico van vertrouwen (sectie 8.6). Daarna beoordelen wij in hoeverre er in de praktijk sprake is van vertrouwen (sectie 8.7). Vervolgens behandelen wij de RID (8.8) en gaan dan verder met de drie belangrijkste modaliteiten van interactie tussen de AIVD en de politie, te weten (1) onderlinge afstemming van activiteiten in het AOT (Afstemmingsoverleg Terrorisme) en het IOT (Inlichtingenoverleg Terrorisme) (sectie 8.8), (2) stelselmatige onderlinge informatie-uitwisseling (sectie 8.9) en (3) samenwerking in het kader van de CT-infobox (sectie 8.10). Wij sluiten af met een hoofdstukconclusie en een antwoord op OV4 (sectie 8.11).

8.1 De traditionele conceptuele verhouding tussen de AIVD en de politie

In deze sectie leggen wij de nadruk op de meer abstracte, conceptuele verschillen tussen de veiligheidsdienst en de politie aan de hand van het onderscheid tussen de hoge politie en de lage politie zoals we in hoofdstuk twee hebben beschreven. Vanuit een korte herhaling van de verschillen kunnen wij de ontwikkelingen goed beschrijven. We beperken ons tot de volgende vier onderwerpen: (1) taak, (2) middel, (3) werkproces, en (4) relatie met externen.

Met betrekking tot (1) de taak (het doel) van de diensten geldt dat de veiligheidsdiensten zijn belast met de bescherming van de nationale veiligheid: het is in dat opzicht een *politieke* politie. De politie is belast met de handhaving van de rechtsorde, oftewel het bestrijden van criminaliteit. Traditioneel richten de veiligheidsdiensten zich op onderwerpen als terrorisme, politiek geweld en activisme. Het gaat om onderwerpen die een bedreiging van de nationale veiligheid opleveren. Het is doorgaans aan de diensten zelf om te bepalen welke gevallen een bedreiging van de nationale veiligheid kunnen opleveren: er is in de meeste landen geen limitatieve opsomming van gedragingen die een bedreiging van de nationale veiligheid vormen. De politie richt zich daarentegen op criminaliteit. Het gaat dan om

[268] Omdat de meeste bevindingen in dit hoofdstuk voor zowel de CIE als de RIO gelden, hanteren wij in het vervolg de schrijfwijze 'CIE/RIO' wanneer de bevindingen voor beide organisatieonderdelen gelden.

gedragingen die te classificeren zijn als strafbare feiten. De categorie van handelingen die een strafbaar feit opleveren is traditioneel beperkt tot de gevallen die in een wetboek van strafrecht (of andere, vergelijkbare wetgeving) zijn opgenomen. De politie kan niet zelfstandig bepaalde gedragingen strafbaar stellen. Deze verschillen in taakstelling leiden ook tot verschillen in (2) het middel waarmee de diensten hun doel proberen te bereiken. De veiligheidsdiensten doen aan risico-inschattingen. De opbouw en instandhouding van een informatiepositie spelen bij de veiligheidsdiensten een grote rol. Zij geven voorwaarschuwingen en focussen zich daarbij op de toekomst. Politiediensten daarentegen zijn traditioneel belast met het vaststellen van de strafrechtelijke waarheid, en zij zijn met name gericht op wat er met betrekking tot strafbare feiten is gebeurd. Zij kijken dus naar het verleden en verzamelen bewijs omtrent wat er is gebeurd. Dit heeft geleid tot verschillen in (3) de werkprocessen. De veiligheidsdiensten maken gebruik van intelligence als werkproces, hetgeen grafisch goed wordt weergegeven met de intelligence-cyclus (zie sectie 2.4). De politie hanteert het opsporingsproces, hetgeen in verregaande mate is gereguleerd. Het laatste verschil tussen de organisaties betreft (4) de relatie van de organisatie met de buitenwereld. Veiligheidsdiensten betrachten een verregaande geheimhouding en schermen hun methoden, bronnen en informatiepositie af van de buitenwereld. De politie daarentegen kent een verregaande mate van transparantie. Er komt een moment waarop de politie (door tussenkomst van een officier van justitie) voor een strafrechter openheid van zaken dient te geven.[269] Schematisch weergegeven zien de verschillen tussen de diensten er als volgt uit.

Dienst	**Veiligheidsdienst (HP)**	**Politie (LP)**
Taak	Nationale Veiligheid	Rechtsorde
Middel	Voorwaarschuwing: Opbouw / instandhouding informatiepositie	Waarheidsvinding: verzamelen bewijs
Werkproces	Intelligence-cyclus	Opsporing
Relatie externen	Geheimhouding	Transparantie

Figuur 8.1: De traditionele conceptuele verhouding

De traditionele verhouding is echter in de praktijk aan belangrijke veranderingen onderhevig. Deze behandelen wij in de volgende sectie.

8.2 Veranderingen

De traditionele conceptuele verhouding zoals wij die in de vorige sectie hebben geschetst, geldt vandaag de dag (2012) niet meer. Vanaf de jaren ‘90 van de vorige

[269] Het gaat hier om ideaaltypen: in de praktijk zijn er veel voorbeelden te geven van openheid en transparantie van veiligheidsdiensten en geheimhouding door de politie. Een voorbeeld van transparantie bij een veiligheidsdienst is het onderzoek door de Commissie Havermans (2004), waarin de AIVD kritisch werd onderzocht. Een voorbeeld van geheimhouding door de politie zijn de CIE-en die aan verregaande bronafscherming doen. Zie voor de mate van geheimhouding door de AIVD hoofdstuk drie, voor de geheimhouding door de CIE hoofdstuk vier.

eeuw hebben zich belangrijke veranderingen voorgedaan die met name de politie hebben omgevormd en kenmerken hebben gegeven die vergelijkbaar zijn met kenmerken van een hoge politiedienst. We behandelen de belangrijkste veranderingen en de wijze waarop deze in de praktijk hebben geleid tot veranderingen aan de hand van de onderwerpen die ook in de vorige subsectie zijn gebruikt, te weten (1) taak (subsectie 8.2.1), (2) middel (subsectie 8.2.2), (3) werkproces (subsectie 8.2.3), en (4) relatie met externen (subsectie 8.2.4). Verreweg de meeste van alle (conceptuele) veranderingen hebben wij waargenomen bij de politie. De volgens ons meest plausibele verklaring hiervoor is dat veranderingen bij de politie zichtbaar zijn. De politie is in veel opzichten een transparante dienst waarbij bijvoorbeeld nieuwe bevoegdheden tot stand komen via een openbaar wetgevingsproces (overigens geldt dit op zichzelf ook voor de AIVD). Maar ook interne veranderingen zoals reorganisaties en de implementatie van IGP vinden vaak in relatieve openheid plaats. Dat gaat vaak gepaard met de nodige media-aandacht of aandacht vanuit de juridische wetenschap. Interne veranderingen bij veiligheidsdiensten zullen, vanwege de verregaande geheimhouding die deze diensten betrachten, niet snel in de openbaarheid komen.[270] De veranderingen die wij schetsen hebben met name betrekking op de Nederlandse situatie. Voor andere landen geldt dat hier weliswaar vergelijkbare veranderingen kunnen optreden, maar de mate waarin en de concrete invulling van de veranderingen verschilt van land tot land. Ons onderzoek richt zich echter op de Nederlandse praktijk, en het gaat te ver om de buitenlandse situatie in de analyse op te nemen.

Wij betogen dat de veranderingen leiden tot een toenemende noodzaak voor de veiligheidsdiensten en de politie om te gaan samenwerken. Het is een noodzaak die ook doorklinkt in verschillende onderzoeksrapportages die zien op de praktijk van de bestrijding van terrorisme. We besluiten met een korte conclusie en een schematische weergave van de veranderingen (subsectie 8.2.5).

8.2.1 Verandering in taak

Met betrekking tot de algemene taakstelling van de diensten zijn in eerste opzicht weinig veranderingen. De veiligheidsdiensten zijn nog steeds belast met de bescherming van de nationale veiligheid. De politie is ook nog steeds belast met het handhaven van de rechtsorde. Echter, daar waar het gaat om de inhoudelijke invulling van deze taken zijn wel grote veranderingen opgetreden.

De belangrijkste verandering vindt plaats in de aandachtsgebieden van met name de politie. De politie (en daarmee de CIE/RIO) blijft weliswaar gefocust op criminaliteit, maar wat er allemaal tot criminaliteit kan worden gerekend, is vanaf de jaren ‘80 van de vorige eeuw aanzienlijk uitgebreid. Met name de opkomst van het islamitisch terrorisme heeft geleid tot nieuwe vormen van criminaliteit. In de politiepraktijk worden deze terroristische misdrijven ook wel ‘ideologische misdrijven’ genoemd. Wij behandelen in deze subsectie allereerst wat er onder ideologische misdrijven kan worden verstaan. Vervolgens behandelen wij in hoeverre het onderwerp binnen de CIE en de RIO wordt uitgewerkt. Wij besluiten de subsectie met de ondergeschikte rol van de politie ten opzichte van de AIVD als het gaat om de bestrijding van terrorisme.

[270] Zie voor een uitzondering op deze regel de discussie omtrent het streven van de AIVD om zich in toenemende mate op het buitenland te gaan richten, de zogenoemde ‘*forward-defense*’. Zie: https://www.aivd.nl/actueel/@2174/forward-defence/, gezien op 28 november 2011. Zie voor een kritische beschouwing van dit streven van de AIVD Bob de Graaff in de NRC van 30 april 2010.

Een gevolg van het feit dat het onderwerp van terrorisme nieuw is voor de politie, is dat men ook niet precies weet wat er onder valt. Het feit dat een juridische definitie van een terroristisch misdrijf in artikel 83 jo. 83a WvSr is opgenomen (zie Lintz 2007; Van Kempen en Van de Voort 2010: 17 e.v.), heeft niet geleid tot een afgebakende praktijkdefinitie. Het uitgangspunt van de juridische definitie is het terroristische oogmerk (zie artikel 83a WvSr), hetgeen ruimte biedt om verschillende onderwerpen onder terrorisme te scharen. In de praktijk wordt het terroristische oogmerk gelijkgesteld aan een soort ideologisch oogmerk. Misdrijven die niet primair worden gepleegd met als oogmerk een geldelijk gewin (de politiële benadering van georganiseerde criminaliteit), maar die wel in een georganiseerd verband worden gepleegd, worden vrij snel onder de ideologische misdrijven geschaard. Dit leidt ertoe dat een contraterrorisme-team van de politie kan werken op het jihadistisch terrorisme, maar ook op bijvoorbeeld extreem links extremisme, extreem rechts extremisme en Turks nationalisme. Deze onderwerpen zijn vrij specialistisch van aard en vereisen bijzondere kennis en expertise, maar de politie beschikt doorgaans niet over de expertise en de mankracht om op al deze onderwerpen gedegen onderzoek te doen. Daarnaast wijken onderzoeken naar terrorisme ook op een andere manier af van de traditionele onderzoeken naar criminaliteit. Volgens de geïnterviewde respondenten die werkzaam zijn op het werkveld van het contraterrorisme zijn de terrorismeonderzoeken minder 'spannend' en 'dynamisch' dan onderzoeken naar (georganiseerde) criminaliteit. Deze laatste onderzoeken gaan sneller en leiden sneller tot concrete resultaten. Zij beantwoorden meer aan de pragmatische 'doeners-mentaliteit' waar wij in subsectie 7.2.2 over hebben geschreven. Dit brengt ons op het tweede onderwerp van deze subsectie: de uitwerking van terrorismebestrijding binnen de CIE en de RIO. Het (nog steeds) nieuwe onderwerp lijkt als specialistisch taakveld niet makkelijk te worden geaccepteerd binnen de CIE.

Terrorismebestrijding verschilt in belangrijke mate met de opsporing- en bestrijding van (georganiseerde) criminaliteit en het maakt dat weinig politiemensen zich tot het onderwerp voelen aangetrokken. Er is op bepaalde terrorismeafdelingen een behoorlijke doorloop van personeel. Een leidinggevende van een afdeling die is belast met terrorismebestrijding verwoordde het als volgt.

"*In de loop van de tijd is het (qua capaciteit) minder en minder geworden. Er zijn er een aantal weggegaan, het is natuurlijk wel een apart taakveld. Als je gewoon bij de CIE zit en je runt op verdovende middelen dan is dat makkelijker om bronnen te krijgen dan bij ons.*" Interview teamleider CIE (D), november 2009.

De realiteit van de politiële terrorismebestrijding beantwoordt dus niet aan de verwachtingen van veel politiemensen. Dit maakt dat veel CIE-runners na een korte periode besluiten over te stappen naar de meer traditionele onderwerpen. We vervolgen het bovenstaande citaat.

"*(…) bij ons is het natuurlijk niet altijd zo spannend. Je moet heel erg investeren voordat je een informatiepositie hebt en iemand zo ver is dat hij dingen wil zeggen. Plus daarbij komt dat als jij hier naartoe gaat met het idee dat je per jaar twee aanslagen gaat voorkomen, dan gaat je dat niet lukken want die hebben we gelukkig niet. Dus ja, als mensen met een bepaald wild west idee hier naartoe komen… Kijk, met verdovende middelen of Hollandse netwerken worden weleens mensen geliquideerd dan heb je toch meer actie dan bij ons. Wij moeten investeren in het*

contact met iemand, en dan moet je vier keer om de tafel zitten en de vijfde keer heb je pas vertrouwen." Interview teamleider CIE (D), november 2009.

De onderwerpen waar de politie volgens enkele respondenten wel mee uit de voeten kan, zijn bijvoorbeeld witwassen, afpersing en andere min of meer traditionele misdrijven die een faciliterende functie voor terroristische organisaties hebben. Deze onderzoeken verschillen weinig van de traditionele opsporingsonderzoeken naar georganiseerde criminaliteit. Sommige respondenten vragen zich af of de politie zich niet tot die onderwerpen dient te beperken. Er zijn immers naast de politie ook nog andere organisaties die zijn belast met terrorismebestrijding, zoals de AIVD en de MIVD. Volgens sommige respondenten zouden deze organisaties de terrorismebestrijding helemaal moeten overnemen zodat de politie zich kan richten op die taken en aandachtsgebieden waar zij een (min of meer) exclusieve taak heeft. De vraag is echter of deze situatie niet al de praktijk is.

De rol van de politie bij terrorismebestrijding wordt in de praktijk anders ingevuld dan de relevante wet- en regelgeving doet vermoeden. Deze laatste geven de politie namelijk een min of meer zelfstandige rol bij het opsporen en voorkomen van terrorisme. De praktijk laat echter zien dat de politie met name een ondergeschikte rol heeft ten opzichte van de AIVD. Vaak wordt de politie ingeschakeld op het moment dat er daadwerkelijk moet worden ingegrepen en de AIVD niet over de juiste middelen en bevoegdheden beschikt. Dit betekent dat wanneer er bijvoorbeeld daadwerkelijk een reëel gevaar bestaat dat er op korte termijn een aanslag plaatsvindt, de AIVD via het OM de politie inschakelt. Het zijn dan de speciale eenheden van de politie (Dienst Specialistische Interventies, Arrestatie Team) die overgaan tot een eventuele aanhouding. Vaak vindt er voorafgaande aan de aanhouding een politieel (opsporings)onderzoek plaats, waarin doorgaans ook de CIE een rol heeft. De CIE verzamelt dan informatie door middel van het runnen van informanten en analyseert deze informatie al dan niet samen met analisten van het RIO. Het probleem voor de politie is dat de AIVD vaak lang wacht met het uitgeven van een ambtsbericht.[271] De politie wordt op een relatief laat moment ingeschakeld voor het verrichten van een opsporingsonderzoek, hetgeen betekent dat het onderzoek dat plaatsvindt lijdt aan tijdsgebrek en kwalitatief van minder hoog niveau is dan gebruikelijk is. Dit heeft weer invloed op de kwaliteit van de CIE-informatie en het latere bewijs, wat volgens veel medewerkers de directe oorzaak is voor de tegenvallende resultaten van de politie in terrorisme-onderzoeken.

Vrijwel alle respondenten geven aan dat de politie en de AIVD steeds meer in elkaars vaarwater komen en dat dit komt omdat de politie zich in toenemende mate bezighoudt met terrorismebestrijding (zie ook Commissie Havermans 2004: 104-105; Adviescommissie Informatiestromen Veiligheid 2006: 67). De organisaties komen elkaar in toenemende mate in operationele zaken tegen (dus in die zaken waarin de AIVD geen ambtsbericht heeft verstuurd). Het gevolg is dat de politie in een vroeg stadium AIVD-agenten in beeld kan krijgen, zonder dat zij zich hiervan bewust is. De agenten zijn voor de politie 'gewoon' verdachten van strafbare feiten, en het gevolg kan zijn dat ze onderwerp worden van een opsporingsonderzoek en bijvoorbeeld aangehouden kunnen worden. Voor de AIVD betekent dit dat er een informatiepositie

[271] Dit gebeurt niet zonder reden. In bepaalde gevallen heeft de AIVD een inlichtingenbelang dat prevaleert aan de belangen van de politie. En alhoewel dit begrijpelijk (en legitiem) is, is het ook begrijpelijk dat de politie doorgaans moeite heeft met deze gang van zaken. Zij voelt zich een speelbal van de AIVD en andere partijen, en krijgt niet de gelegenheid om een gedegen opsporingsonderzoek uit te voeren.

verloren gaat, hetgeen tot gevolg kan hebben dat de dienst geen tijdige voorwaarschuwingen kan geven over mogelijke op handen zijnde terroristische activiteiten. Dit vereist dus dat er communicatie is tussen de organisaties en dat de activiteiten onderling worden afgestemd. In de volgende sectie behandelen we de wijze waarop de organisaties reageren op deze nieuwe werkelijkheid.

De hiervoor behandelde constatering van de respondenten lijkt in tegenspraak met het voorgaande, waarin wij betoogden dat de veranderingen in werkmethoden en processen binnen de CIE/RIO in de praktijk nog nauwelijks zijn doorgevoerd (zie hoofdstuk zeven). Dit is echter niet het geval. Terrorismebestrijding is een nieuw onderwerp voor de politie in het algemeen en de CIE/RIO in het bijzonder. En ondanks het gegeven dat terrorismebestrijding binnen de CIE/RIO nog nauwelijks is geaccepteerd, verricht de CIE/RIO wel activiteiten op het gebied van terrorismebestrijding. Door de CIE worden potentiële nieuwe informanten aangelopen en langzaamaan wordt er een informantenbestand en informatiepositie op terrorisme opgebouwd. In het kader van dit nieuwe onderwerp komen de AIVD en de CIE/RIO elkaar aldus in operationele onderzoeken tegen. De werkzaamheden en werkprocessen van de CIE/RIO met betrekking tot terrorismebestrijding vinden echter nog grotendeels op de traditionele wijze plaats: reactief, gericht op waarheidsvinding en volgens het opsporingsproces. Dat de CIE/RIO niet volgens IGP (en daarmee het concept van intelligence) werkt, betekent derhalve niet dat de AIVD en de CIE/RIO elkaar niet vaker in een operationele context zullen tegenkomen. Ook werkend volgens de traditionele werkmethoden kan de CIE/RIO inlichtingentrajecten van de AIVD doorkruisen en beschadigen. Dit vereist voorts een goede afstemming, informatie-uitwisseling en onderlinge samenwerking.

8.2.2 Verandering in middel

Voor de veiligheidsdiensten hebben wij geen veranderingen kunnen vaststellen van het middel waarmee zij hun taak uitvoeren. Dit is op zichzelf ook niet vreemd, veiligheidsdiensten zullen altijd moeten proberen om risico's in te schatten en kunnen het zich niet veroorloven om het primaat van de werkzaamheden opeens bij reactieve waarheidsvinding neer te leggen. Alleen in technologisch opzicht zijn er wel veranderingen geweest. Het gaat hierbij om aanpassingen aan de moderne technologie, maar dit waren geen conceptuele veranderingen. Bij de politie hebben wij daarentegen wel een belangrijke verschuiving waargenomen.

Zoals wij in hoofdstuk vijf hebben beschreven, stelt de risicosamenleving nieuwe eisen aan de politie. Zij moet in toenemende mate aan risico-inschattingen gaan doen en proberen criminaliteit te voorkomen. De politie zal niet alleen bewijs moeten verzamelen en aan waarheidsvinding moeten gaan doen, maar moet ook overgaan tot het opbouwen en in stand houden van een informatiepositie. Risico-inschattingen vereisen immers een hele andere benadering van het verzamelen en analyseren van informatie dan onderzoeken naar de materiële strafrechtelijk relevante waarheid. Deze verschuiving is in de praktijk duidelijk waarneembaar, in ieder geval daar waar het gaat om de juridische mogelijkheden met betrekking tot het verzamelen en verwerken van informatie. We behandelen hieronder eerst de meest relevante juridische ontwikkelingen, bestaande uit (A) de themaverwerkingen uit de WPG en (B) het verzamelen van informatie door de toepassing van 'lichte' BOB-bevoegdheden in de CIE-fase. Na de juridische ontwikkelingen bezien we (C) in hoeverre deze ontwikkelingen in de praktijk daadwerkelijk worden gebruikt.

A: Themaverwerkingen

Sinds het begin van de WPG (1 januari 2008) zien we nieuwe verwerkingsmodaliteiten die primair als doel hebben de zelfstandige opbouw en instandhouding van een informatiepositie mogelijk te maken. Het gaat dan om de zogenaamde 'themaverwerkingen' van artikel 10 lid 1 sub b WPG (zie CBP 2005 voor een kritische beschouwing van de themaverwerkingen). Themaverwerkingen bieden op bepaalde door AMvB vastgestelde thema's een ruimere mogelijkheid voor het verwerken van gegevens omtrent personen. De thema's zijn terrorisme, mensenhandel en mensensmokkel. De Memorie van Toelichting (MvT) stelt omtrent de themaverwerking het volgende: "(een themaverwerking) *betreft de gegevensverwerking teneinde inzicht te verkrijgen in de betrokkenheid van personen bij handelingen die kunnen wijzen op het beramen of plegen van misdrijven die (…) een ernstig gevaar voor de rechtsorde opleveren. De aanpak van deze misdrijven vergt de opbouw en instandhouding van een permanente informatiepositie.*"[272] De MvT stelt voorts dat op deze zwaarwegende thema's de klassieke strafrechtelijke benadering niet afdoende is en dat om "*deze dreigingen het hoofd te kunnen bieden en inzicht te kunnen verkrijgen in de kring van personen die (…) daarbij betrokken kunnen zijn*" informatie verzameld en geanalyseerd dient te worden.[273] Op het gebied van terrorisme, mensenhandel en mensensmokkel heeft de wetgever de ontwikkeling naar risico-inschattingen dus duidelijk verwoord. Op de genoemde thema's heeft de politie een positie die vergelijkbaar is met die van de veiligheidsdiensten. Overigens wordt een themaverwerking niet noodzakelijkerwijs door een CIE gedaan. Dit is wel mogelijk, doch het is ook mogelijk dat er een andere eenheid of team specifiek met het uitvoeren van de themaverwerking wordt belast (zie artikel 2:4 Bpolg).

B: BOB-bevoegdheden in de CIE-fase

De themaverwerkingen zien op het verwerken van gegevens. Dit is slechts een deel van het informatieproces. Om te bezien in hoeverre het opbouwen en in stand houden van de informatiepositie door de politie lijkt op die van de veiligheidsdiensten is het ook van belang om de praktijk van de informatieverzameling nader te beschouwen. Zoals in subsectie 4.4.2 al is gesteld, bestaat er bij de CIE-officieren van justitie het beeld dat bepaalde BOB-middelen mogen worden ingezet in de 'intelligence-fase', oftewel de CIE-fase voorafgaand aan de uitvoering van het concrete opsporingsonderzoek in de zin van artikel 132a WvSv. Met 'intelligence' doelen de officieren overigens op start- en sturingsinformatie (zie subsectie 4.4.2). Dit is de zoveelste definitie van intelligence die binnen het domein van de opsporing wordt gehanteerd, hetgeen verwarrend is voor de diverse bij de opsporing betrokken partijen. Het is voor ons onderzoek van belang om na te gaan in hoeverre er in de praktijk daadwerkelijk gebruik wordt gemaakt van BOB-middelen. Indien in de CIE-fase BOB-middelen worden toegepast, dan is de kans aanwezig dat deze toepassing geschiedt met als doel de opbouw en instandhouding van een informatiepositie. Dit brengt de werkwijze van de CIE (en de politie in het algemeen) dichter bij die van de veiligheidsdiensten.

[272] *Kamerstukken II* 2005-06, 30 327, nr. 3, p. 48.
[273] *Ibid*.

C: Weinig veranderingen in de praktijk

We hebben eerder en kort hierboven de juridische ontwikkelingen met betrekking tot de verwerking en verzameling van informatie behandeld. De vraag die rijst, is in hoeverre de ruimte die de bovengenoemde juridische ontwikkelingen de CIE en de RIO bieden, in de praktijk daadwerkelijk wordt gebruikt. We beginnen met de themaverwerkingen.

De themaverwerkingen worden in de praktijk van de politiële terrorismebestrijding toegepast. Wij hebben tijdens ons veldwerk dan ook herhaaldelijke discussies over de themaverwerkingen meegemaakt. De politiemedewerkers op het gebied van terrorismebestrijding zijn doorgaans enthousiast over de mogelijkheden van de themaverwerking en zien het als een duidelijke verbetering voor de informatiehuishouding van de politie. Wat ons echter opviel, was dat de ruime mogelijkheden die de themaverwerkingen bieden er in de praktijk toe leiden dat erg veel informatie in de bestanden wordt opgeslagen met als redenering dat het mogelijk in de toekomst van belang zou kunnen zijn. Dit past binnen een risicobenadering, van tevoren is het immers moeilijk inschatten welke informatie wel en welke informatie niet van belang zou kunnen zijn. Het neveneffect hiervan is echter dat de informatiebestanden in korte tijd heel erg groot worden en dat veel informatie eigenlijk van relatief lage waarde is: hier bestaat het risico van *data-overload* (Sheptycki 2004; zie ook subsectie 7.6.2). Dit komt onzes inziens mede omdat er geen moment meer is waarop de informatie kritisch wordt beoordeeld alvorens deze wordt opgeslagen: bij twijfel wordt informatie opgeslagen. De wet biedt daartoe immers de ruimte, en 'je zou wel gek zijn als je deze ruimte niet zou gebruiken'. Een vergelijkbaar probleem speelt met de CIE-gegevens in de themabestanden. In de praktijk wordt (begrijpelijk) vaak aangevoerd dat themaverwerkingen als doel hebben het opbouwen en in stand houden van de informatiepositie, en dat CIE-informatie daarvoor ook van belang is. Het is overigens geen automatisme dat informatie uit de CIE-bestanden automatisch moeten worden opgenomen in de themabestanden. De afscherming van de CIE-informatie geldt ook in het geval van de themaverwerkingen.

De ruimere mogelijkheden van de themaverwerkingen leiden er overigens ook toe dat sommige politiemedewerkers geneigd zijn om zelfstandig onderwerpen te benoemen als thema. Zij redeneren dat alles met betrekking tot georganiseerde criminaliteit een ernstig gevaar voor de rechtsorde oplevert en dat dit daarmee de opbouw en instandhouding van een permanente informatiepositie vereist. Dit maakt dat ook voor andere onderwerpen dan de bij besluit vastgestelde (terrorisme, mensenhandel en mensensmokkel) geldt dat er sprake is van een thema als bedoeld in artikel 10 lid 1 sub b WPG. Om te kunnen spreken van een thema in de zin van de WPG, dient het thema echter bij AMvB te zijn vastgesteld. De bestanden die zien op andere dan de bij AMVB genoemde onderwerpen zullen moeten worden gevoerd onder het regime van artikel 8, 9 of 10 lid 1 sub a WPG. Wij hebben elders reeds vraagtekens gezet bij de neiging van opsporingsorganisaties om als een soort stofzuiger ongebreideld informatie te verzamelen: er zal immers een bepaalde filter moeten worden gebruikt om informatie-*overload* te voorkomen en om niet in strijd met relevante rechtsbeginselen zoals privacy en dataprotectie te werken (zie De Hert en Vis 2005; zie voor een kritische beschouwing van politiële gegevensverwerking en privacy ook: Kielman 2010). Voorheen was dit primair een kenmerk van de hoge politie, de veiligheidsdiensten. Nu de politie zich ook probeert te richten op de toekomst en de opbouw en instandhouding van de informatiepositie, stellen wij vast

dat zij met betrekking tot dit kenmerk in toenemende mate op een hoge politie gaat lijken.

Met betrekking tot het verzamelen van informatie constateren wij echter dat politie en justitie veel minder gebruik maken van nieuwe, proactieve mogelijkheden. In het verleden is gebleken dat bij bepaalde juridische verruimingen de politiepraktijk (en justitie) terughoudend is met het verkennen van de nieuwe mogelijkheden (zie Beijer et al. 2004; zie over de toepassing van terrorismewetgeving ook Van Gestel et al. 2009: 45 e.v.). Wij constateren dat dit eveneens geldt voor onderzoeken naar terroristische misdrijven. Tijdens ons onderzoek is ons slechts één geval gebleken waarin BOB-bevoegdheden op basis van een aanwijzing zijn ingezet. Onder de huidige anti-terrorismewetgeving is een aanwijzing dat iemand mogelijk is betrokken bij terroristische misdrijven voldoende om een opsporingsonderzoek op te starten en bijzondere opsporingsbevoegdheden in te zetten. In dat onderzoek is men snel overgegaan tot de meer traditionele bevoegdheden omdat er spoedig een verdenking in de zin van artikel 27 WvSv was. Uit een monitor van het WODC blijkt voorts dat in de periode februari 2009 tot en met februari 2010 in slechts vier van de 31 onderzoeken naar terrorisme van de nieuwe bevoegdheden gebruik is gemaakt (zie Van Gestel, De Poot en Kouwenberg 2010). De politie (en niet te vergeten justitie) lijkt dus niet geneigd om snel deze nieuwe mogelijkheden toe te passen. Voorts verwijzen wij naar hoofdstuk zeven. Daarin hebben wij reeds geconcludeerd dat de CIE nog steeds reactief te werk gaat. Er zijn weliswaar veel ideeën en initiatieven die uitgaan van een proactieve informatieverzameling en een permanente opbouw van een informatiepositie, maar in de praktijk is hier nog weinig van terecht gekomen. Er wordt dan ook met name geëxperimenteerd met risico- en dreiginginschattingen, wat doorgaans in *pilot-settings* gebeurt. Maar van een operationele toepassing in de praktijk is geen sprake. De wens om aan risico-inschattingen te doen en de daarbij noodzakelijke informatiepositie op te bouwen is er wel, maar de praktijk van het politiewerk lijkt daar (nog) niet aan te kunnen voldoen. Wij concluderen dan ook dat op dit tweede verschil tussen de organisaties (verandering in middel) weliswaar een conceptuele en theoretische verschuiving heeft plaatsgevonden, maar dat ook hiervoor geldt dat de verschuiving in de praktijk van de CIE niet optreedt. De CIE blijft in dit opzicht een lage politie.

Met betrekking tot de praktijk van de toepassing van BOB-bevoegdheden in de CIE-fase (zie subsectie 4.3.2) hebben we van een klein aantal respondenten vernomen dat men erg terughoudend is met het toepassen ervan. Er wordt door CIE-ers en CIE-officieren van justitie een onderscheid tussen zware en minder zware BOB-bevoegdheden gemaakt. Zware BOB-bevoegdheden maken volgens deze betrokkenen een verregaande inbreuk op de persoonlijke levenssfeer, en minder zware BOB-bevoegdheden maken een beperkte inbreuk op de persoonlijke levenssfeer. Een zware BOB-bevoegdheid is bijvoorbeeld de telefoontap. De minder zware BOB-bevoegdheden zijn die uit de Wet Bevoegdheden Vorderen Gegevens.[274] Deze minder zware bevoegdheden worden in de praktijk ook wel aangeduid als *BOB-light*. Wij merken voor de duidelijkheid op dat dit onderscheid tussen zware en minder zware BOB-bevoegdheden een praktijkonderscheid is: de wetgever spreekt van BOB-bevoegdheden en brengt in dit opzicht geen onderscheid aan tussen zware en minder zware varianten. De reden voor het praktijkonderscheid ligt in het feit dat de *BOB-light* bevoegdheden voor de inwerkingtreding van de Wet Bevoegdheid Vorderen Gegevens op 1 januari 2006 al werden toegepast (op basis van artikel 2 Politiewet

[274] Wet van 16 juli 2005, Stb. 2005, 390, in werking getreden op 1 januari 2006.

1993). Nu ze in het Wetboek van Strafvordering zijn opgenomen, gelden er striktere bepalingen omtrent de toepassing ervan. Volgens CIE-ers en CIE-officieren van justitie is toepassing van deze bevoegdheden in de CIE-fase mogelijk, omdat dit voor de inwerkingtreding van de Wet Bevoegdheid Vorderen Gegevens ook al mogelijk was op basis van artikel 2 Politiewet 1993 (Van der Bel et al. 2009: 165). Met name van de bevoegdheid om historische gegevens van bijvoorbeeld een telefoonmaatschappij op te vragen (artikelen 126nd t/m 126ud WvSv) wordt zeer summier in de CIE-fase toegepast. Dit wordt echter doorgaans gedaan ter controle van een informant en ter verkrijging van start- en sturingsinformatie. Op basis van die gegevens kan worden nagegaan of de informant daadwerkelijk daar is geweest waar hij zegt te zijn geweest. Deze toepassing is begrijpelijk en kan ook in het belang van CIE-subjecten en verdachten zijn. Immers, hoe valt anders een informant te controleren door een CIE? Hier hebben CIE-subjecten en verdachten ook belang bij. Het argument waarom deze lichte BOB-middelen in de CIE-fase kunnen worden toegepast, is dat dezelfde bevoegdheden voordat ze in de Wet BOB zijn opgenomen reeds binnen de CIE-fase werden (en mochten worden) toegepast, en dit zou dus in de huidige situatie ook moeten kunnen. De redenering is voorts dat de inbreuk op de persoonlijke levenssfeer niet groter is geworden dan toen de bevoegdheid werd toegepast op basis van artikel 2 Politiewet 1993. Het staat overigens buiten discussie dat de CIE geen BOB-bevoegdheden kan inzetten om bewijs te verzamelen (zie Van der Bel et al. 2009: 165-166).

Wij hebben niet kunnen vaststellen dat BOB-bevoegdheden door de tactische opsporingsteams worden ingezet met als doel het opbouwen en in stand houden van een informatiepositie, met uitzondering van de bevoegdheden in het kader van de bestrijding van terrorisme. Wij hebben met één opsporingsonderzoek naar terroristische misdrijven meegewerkt. Het doel van de opsporing van terroristische misdrijven is volgens de wetgever niet alleen het hard maken van een redelijke verdenking, maar minstens evenzeer het voorkomen van een mogelijke aanslag. Het voorkomen van een aanslag is dus de achterliggende gedachte bij de toepassing van BOB-bevoegdheden in het kader van terroristische misdrijven. Bij het voorkomen van terroristische aanslagen kijkt men naar de toekomst en hiervoor is het opbouwen en in stand houden van een informatiepositie onontbeerlijk. In het onderzoek waaraan wij hebben meegewerkt lag de nadruk ook daadwerkelijk op het voorkomen van aanslagen, en alle inspanningen (waaronder de inzet van BOB-bevoegdheden) waren daarop gericht. Wij merken hierbij echter op dat dit in zekere zin een zeer reactief onderzoek was. Er was een ambtsbericht van de AIVD waarin personen werden aangemerkt als mogelijke leden van een jihadistisch netwerk en de politie was er met name op gericht om deze personen zoveel mogelijk onder controle te houden. De AIVD had de voorwaarschuwing al gegeven, en de mogelijke verdachten waren voor de politie daarmee al bekend. Er was dus al een dreiging: alle signalen stonden op rood. De informatie-inwinning was derhalve gericht op het verzamelen van zoveel mogelijk actuele, *up to date* informatie zodat er direct kon worden ingegrepen mocht dat nodig zijn. Voor de politie was er in dit opzicht geen noodzaak meer voor een intelligence-benadering waarin zij zelf dreigingen identificeert en vervolgens tot opsporing over gaat. De dreiginginschattingen die binnen het politiële onderzoek plaatsvonden waren gericht op het duiden van de actuele situatie en het beantwoorden van de vraag 'wat gebeurt er nu?' De informatie-inwinning had als doel het opbouwen en in stand houden van een informatiepositie, maar niet ten behoeve van een intelligence-benadering. Dergelijke politiële onderzoeken naar terrorisme die worden geïnitieerd door een ambtsbericht zijn in belangrijke mate dus reactieve onderzoeken

die veel gelijkenis vertonen met de klassieke opsporingsonderzoeken. In hoeverre dit voor de politiële bestrijding van terrorisme in het algemeen opgaat, kunnen wij op basis van ons onderzoek niet stellen. Wij hebben immers slechts één onderzoek onderzocht. Daarnaast merken wij op dat deze tactische opsporing van terroristische misdrijven niet door de CIE of RIO wordt verricht, maar door tactische opsporingsteams. De CIE en de RIO ondersteunen een dergelijk onderzoek, maar de inzet van BOB-bevoegdheden ligt geheel bij de tactische opsporingsteams. De tactische opsporing valt buiten de scope van ons onderzoek en dit laten we dan ook verder buiten beschouwing. Wij volstaan met de opmerking dat het waarschijnlijk is dat onderzoeken naar terroristische misdrijven die worden gestart op basis van een AIVD-ambtsbericht doorgaans veel gelijkenis zullen vertonen met traditionele opsporingsonderzoeken.

Wij concluderen met betrekking tot het tweede verschil tussen de politie en de veiligheidsdienst (het verschil in middel) dat in juridisch opzicht er veel lijkt te zijn veranderd in de verhouding tussen de CIE/RIO en de AIVD. De politie richt zich in toenemende mate op de opbouw en in standhouding van de informatiepositie, en krijgt daarvoor ook de benodigde juridische middelen en mogelijkheden. In de praktijk is de verhouding echter nauwelijks veranderd. Er is een vrij grote terughoudendheid bij politie en justitie in het algemeen als het gaat om het benutten van nieuwe juridische mogelijkheden. Alleen daar waar het gaat om het verwerken van informatie wordt er gebruik gemaakt van de nieuwe mogelijkheden die de themaverwerkingen bieden. Het verzamelen van informatie gebeurt echter nog steeds op de traditionele wijze. De CIE/RIO werken in zeker opzicht nog primair als een traditionele, reactieve lage politiedienst.

8.2.3 Veranderingen in het werkproces

Hieronder bezien we de veranderingen met betrekking tot het werkproces. Wij kunnen hier kort over zijn omdat dit voor een groot deel het onderwerp van hoofdstuk zeven (en in mindere mate hoofdstuk vijf) is geweest. Onder invloed van IGP zou de politie in toenemende mate werken volgens het intelligenceproces (de intelligence-cyclus). We hebben in hoofdstuk zeven gezien dat dit in de praktijk echter nog niet echt van de grond komt. Er is dus nog geen sprake van een intelligencegestuurde politie die volgens de intelligence-cyclus werkt. Er is geen sprake van een vraaggestuurde politieorganisatie, maar veel meer van een organisatie die vanuit een waan van de dag werkt. Dit betekent overigens niet dat er in de toekomst geen sprake zal zijn van een politie die werkt volgens IGP: de politie werkt hard aan het realiseren van een aantal randvoorwaarden, en als ze daarin slaagt zal het verschil tussen de werkprocessen van politie en AIVD (veel) kleiner worden.

8.2.4 Veranderingen in de relatie met externen?

Met betrekking tot mogelijke veranderingen in de context van de CIE kunnen wij ook kort zijn. Zoals reeds in hoofdstuk twee is gesteld, is de politie met name een transparante organisatie en kent een veiligheidsdienst als de AIVD daarentegen een veel grotere mate van geheimhouding. De CIE kent echter traditioneel ook een verregaande geheimhouding, dit vanwege de afscherming van de identiteit van de informanten. In deze situatie zijn geen veranderingen opgetreden. De AIVD is nog steeds een organisatie die verregaande geheimhouding betracht tegenover de buitenwereld, en dit geldt ook voor de CIE. Waar wel veranderingen in zijn

opgetreden, is in het *need to share* streven. Het lijkt erop dat de politie intern in toenemende mate transparanter is geworden, hetgeen bij de AIVD nog meer de vraag kan oproepen in hoeverre de politie in staat is om informatie geheim te houden. Maar bij de CIE lijkt *need to share* anno 2012 nog weinig voeten aan de grond te krijgen (zie hoofdstuk zeven). Wij laten dit onderwerp met betrekking tot de conceptuele verhouding dan ook verder buiten beschouwing. Bij de behandeling van het onderwerp van vertrouwen komt geheimhouding wel uitgebreid aan bod (zie sectie 8.6).

8.2.5 Tussenconclusie

In deze sectie hebben we de veranderingen in de verhouding aan de hand van de verschillen tussen de AIVD en de politie behandeld. Ondanks het feit dat deze veranderingen in de praktijk minder vergaand zijn dan in theorie, geven ze wel duidelijk aan dat er belangrijke ontwikkelingen in de verhouding tussen de organisaties plaatsvinden. Met name de politie lijkt in toenemende mate de kenmerken van de AIVD over te nemen en verandert langzaam (in theorie) van een lage politie in een hoge politie. In figuur 8.2 zijn de veranderingen schematisch weergegeven in gecursiveerde vorm.

Dienst	**AIVD (HP)**	**Politie (LP)**
Taak	Nationale Veiligheid: Terrorisme, gewelddadig (politiek) activisme	Rechtsorde: Criminaliteit + *ideologische misdrijven*
Middel	Voorwaarschuwing: Opbouw & instandhouding informatiepositie	Waarheidsvinding: verzamelen bewijs + *voorwaarschuwing / opbouw & instandhouding informatiepositie*
Werkproces	Intelligence-cyclus	Opsporing + *intelligence-cyclus*
Relatie externen	Geheimhouding	Transparantie

Figuur 8.2: veranderingen in de verhouding

Ondanks het feit dat de organisaties in theorie in toenemende mate op elkaar lijken, blijven de organisaties toch van elkaar gescheiden. Het zijn twee verschillende organisaties met elk een eigen taakstelling, maar die taakstellingen gaan steeds meer op elkaar lijken qua doelstelling (het geven van voorwaarschuwingen) en werkproces (intelligence) en ze gaan zich ook nog eens op hetzelfde aandachtsgebied richten. In rechtsstatelijke zin is de scheiding evenwel absoluut: opsporings- en veiligheidsdiensten dienen van elkaar gescheiden te blijven. Er bestaat dus nog steeds een juridische en organisatorische muur tussen beide organisaties. Door deze organisaties gescheiden te houden maar wel vergelijkbare taken te geven op dezelfde onderwerpen, is de kans groot dat ze gaan concurreren om bijvoorbeeld invloed en budgetten (zie ook Peters 2001: 226). Er zijn meerdere scenario's denkbaar over wat de ongewenste gevolgen hiervan kunnen zijn voor de werkverhouding tussen de

organisaties. Wij noemen er twee. Zo is het (1) mogelijk dat de organisaties concurrenten worden met alle negatieve gevolgen voor de bestrijding van terrorisme in het algemeen (informatie wordt bijvoorbeeld afgeschermd, of de activiteiten van de concurrent worden opzettelijk tegengewerkt). Diverse respondenten bestempelen de huidige verhouding als één van concurrentie. Het is ook mogelijk dat (2) beide organisaties naast elkaar bestaan en functioneren en zich onderling niet of nauwelijks met elkaar bemoeien. Het gevolg zou kunnen zijn dat ze elkaar onopzettelijk tegenwerken, bijvoorbeeld doordat de politie agenten van de AIVD gaat aanhouden en zo de informatiepositie van de dienst beschadigt. Deze twee scenario's zijn beide voor de terrorismebestrijding in het algemeen onwenselijk. Uit verschillende evaluaties van het falen van organisaties bij de bestrijding van terrorisme blijkt dat beide situaties bijvoorbeeld leiden tot gebrekkige informatie-uitwisseling met als gevolg dat terroristische aanslagen plaatsvinden die eigenlijk voorkomen hadden kunnen worden (Turner 2004; Phythian 2006: 103-123). Een respondent verwoordde het als volgt.

"*We lopen elkaar nu bewust of onbewust toch echt voor de voeten. Het doel is Nederland veiliger maken, aanslagen te voorkomen. Om dit te bereiken moeten we meer communiceren, en misschien moet er wat wetgeving gaan veranderen waardoor wij beter de zaken kunnen afschermen. Dan creëer je meer ruimte om met elkaar samen te werken.*" Interview runner CIE (B), oktober 2008.

Om niet in een dergelijke onwenselijke bureaupolitiek en onderlinge concurrentie te vervallen, is het noodzakelijk dat de AIVD en de CIE/RIO de interactie opzoeken (zie ook Commissie Havermans 2004: 205; Adviescommissie Informatiestromen Veiligheid 2006: 69). Wij maken een onderscheid in drie modaliteiten van interactie, en plaatsen ze in een rangschikking gebaseerd op de mate van vertrouwen die is vereist. Zo is er (1) de afstemming van activiteiten. Dit is de minst verregaande vorm van interactie, en dit vereist het minste onderlinge vertrouwen. Een andere, meer verregaande modaliteit is (2) stelselmatige onderlinge informatie-uitwisseling. In principe is het delen van informatie een onderdeel van alle modaliteiten van samenwerking. Zo wordt er bij afstemming van werkzaamheden ook informatie gedeeld, omdat dit nu eenmaal nodig is om werkzaamheden af te kunnen stemmen. Maar dit gebeurt doorgaans op ad hoc basis, wanneer er een specifieke aanleiding tot afstemming nodig is. Stelselmatige informatie-uitwisseling gaat verder dan dat. Het betekent dat informatie wordt uitgewisseld ongeacht of daar een specifieke aanleiding voor is. Dit vergt meer vertrouwen in de andere partij. De meest verregaande modaliteit is (3) een onderlinge samenwerking. Voor een succesvolle samenwerking is het meeste vertrouwen nodig, omdat sprake is van een wederzijdse afhankelijkheid . Dit betekent onder andere dat er veel informatie onderling gedeeld moet worden en dat geheimhouding tot een minimum moet worden beperkt.

Een essentieel onderdeel van alle drie de vormen van interactie is dat er sprake is van een bepaalde mate van vertrouwen. Er wordt echter te vaak gesteld dat de organisaties elkaar moeten vertrouwen, zonder dat men analyseert wat vertrouwen is en wanneer er al dan niet aan kan worden voldaan (zie Havermans 2004; Adviescommissie Informatiestromen Veiligheid 2006: 63, 67-69). In sectie 8.3 behandelen wij het concept vertrouwen. Na de secties over het onderwerp vertrouwen (sectie 8.3 tot en met 8.7), zullen wij de hierboven genoemde modaliteiten van interactie bestuderen aan de hand van concrete voorbeelden uit ons veldwerkonderzoek.

8.3 Vertrouwen

De AIVD en de politie worden geconfronteerd met een nieuwe werkelijkheid en dus met nieuwe uitdagingen. Er wordt van ze verwacht dat ze informatie uitwisselen, activiteiten afstemmen en samenwerken. Volgens de commissie Havermans zouden er "(…) *meer organisatorische, personele en formele mogelijkheden moeten worden gecreëerd om de informatievergaring van de AIVD en die van de politie op een rechtens aanvaardbare wijze op elkaar af te stemmen.*" (Commissie Havermans 2004: 107). Er is dus volgens deze commissie genoeg reden om samen te werken en dus een duurzame(re) relatie tussen beide actoren tot stand te brengen.

Wij beginnen eerst met wat de respondenten zeggen over het onderlinge vertrouwen tussen de AIVD en de politie wanneer ze daar direct naar worden gevraagd (subsectie 8.3.1). Daarna staan wij in subsectie 8.3.2 stil bij het concept van vertrouwen. Wat is het precies, op welke manier komt het tot stand en wat zijn belemmeringen voor vertrouwen?

8.3.1 Onderling vertrouwen volgens respondenten

De Commissie Havermans (2004: 45) stelde vast dat de partners van de AIVD (inclusief de politie) een negatief beeld van de AIVD hebben. De terughoudendheid van de AIVD om informatie die in de ambtsberichten is opgenomen aan te vullen met andere relevante informatie trekt een zware wissel op het vertrouwen van het OM in de AIVD, aldus de Commissie Havermans (2004: 106).[275] De vraag die in het kader van ons onderzoek relevant is, is of er tussen de CIE/RIO en de AIVD sprake is van vertrouwen. Diverse respondenten geven hieromtrent aan dat vertrouwen absoluut noodzakelijk is voor een efficiënte bestrijding van terrorisme. Hierover bestaat vrijwel geen verschil van mening. Op de vraag of de respondenten de AIVD vertrouwen, komen veel uiteenlopende antwoorden. In de meeste gevallen geven respondenten aan dat *zij* de dienst in principe wel vertrouwen, maar dat collega's dat doorgaans niet doen. Een duidelijk voorbeeld wordt door een teamleider CIE gegeven.

"*Ik heb daar een dubbel gevoel bij. Bij de (terrorisme-eenheid) is zoals ik al zei helemaal geen vertrouwen in de AIVD. Dat is daar de grootste vijand. Voor mijzelf geldt eigenlijk hetzelfde als ik met andere mensen heb: de ene vertrouw je wat meer dan de ander. Het is niet zo dat ik de mensen van de dienst niet vertrouw, maar ik weet wel dat ze niets alles kunnen zeggen. Dat is lastig. Normaal ben je gewend mensen die je vertrouwt alles te vertellen. Dat kan bij de dienst dus niet. Achteraf, na zo'n IOT* (Inlichtingenoverleg Terrorisme, opmerking auteur)*, bespreken een collega en ik wel hoe het ging en wat de dienst zei. Dan proberen we dat een beetje te plaatsen.*" Interview teamleider CIE (E), november 2010.

Er is vaak ook sprake van negatieve beeldvorming, al dan niet gestoeld op concrete ervaringen. Wanneer gevraagd naar hoe hij de AIVD ziet, is een andere CIE-er erg stellig in zijn mening. Hij zegt over de AIVD het volgende.

[275] Het OM doet het verzoek tot informatie aan de AIVD via de landelijke terrorisme officier van justitie. De politie kan niet buiten deze officier om een informatieverzoek aan de AIVD doen. Verstrekkingen door de AIVD gaan via de landelijke terrorisme officier van justitie naar het OM (zie Van der Bel et al. 2009: 107 e.v.).

"*Het verschil is dat de politie te maken heeft met wetgeving, met allerlei regels. De AIVD heeft geen wet, inlichtingendiensten doen alles wat god verboden heeft. Ja, denk nou maar niet te naïef. Ze halen info binnen, maar hoe dat interesseert ze niet. Ze hebben veel minder procedures, en ik geef toe, soms ben ik wel eens jaloers. En als een doel bereikt moet worden, dan gebeurt dat gewoon, dan gaan ze zich echt niet aan zoiets als regels houden. Het beeld dat CIE-ers hebben over de AIVD is dan ook niet echt positief.*" Interview analist CIE (G), maart 2011.

Het zal duidelijk zijn dat een dergelijk negatief beeld over de AIVD het vertrouwen in diezelfde organisatie niet ten goede komt.

Het beeld dat vaak door diverse respondenten wordt geschetst is dat het probleem van een tekortschietend vertrouwen met name speelt tussen leidinggevenden. Tussen de medewerkers op de werkvloer is de communicatie eigenlijk vaak goed, en is er vrij snel sprake van onderling vertrouwen. Zo vertelde één respondent over een oefening die een CIE samen met een afdeling van de AIVD heeft gedaan het volgende.

"*Dat was echt grappig. Best wel kritisch naar elkaar toe. Ik was met een jongen op pad, een AIVD-er, enne, die zei 'het zou zo mijn maat kunnen zijn'. Dat was wel leuk. En dat was ook zo met die jongen, dat was een goeie jongen.*" Interview teamleider CIE (D), november 2009.

Vertrouwen lijkt dus wel mogelijk tussen de organisaties, mits het op de werkvloer gebeurt. Dit brengt ons op het onderwerp van vertrouwen. Wat is vertrouwen precies en hoe werkt het?

8.3.2 Het concept 'vertrouwen'

Wij behandelen het concept van vertrouwen aan de hand van het theoretische model van Russell Hardin (2006).[276] Hardin stelt dat veel analyses over vertrouwen (*trust*) eigenlijk gaan over betrouwbaarheid (*trustworthiness*): wanneer heeft iemand die kenmerken die ervoor zorgen dat wij hem of haar vertrouwen (Hardin 2006)?[277] Als je iemand vertrouwt, zeg je daarmee eigenlijk dat je gelooft dat de ander de juiste intenties naar jou toe heeft en over de vereiste competenties beschikt om datgene te doen waarmee je hem of haar vertrouwt (Hardin 2006: 17). Dit geloof in de ander is de kern van vertrouwen, en kan op verschillende manieren conceptueel worden benaderd. Volgens Hardin is de beste conceptuele benadering die van de '*encapsulated interests*'.[278] Deze benadering gaat uit van de veronderstelling dat de potentieel vertrouwde persoon belang heeft bij het onderhouden van een relatie met de vertrouwer, en dit belang geeft de vertrouwde persoon de prikkel en het motief om betrouwbaar te zijn. De verwachting van de vertrouwer is dat zijn belangen door de vertrouwde persoon worden ingekapseld in zijn eigen belangen. Van de vertrouwde

[276] Over Hardin en zijn benadering van vertrouwen is eerder door ons geschreven. Deze tekst is op die publicatie gebaseerd. Zie: Vis (2010).

[277] Er zijn veel meer auteurs die iets over vertrouwen hebben geschreven, maar Hardin geeft een goed overzicht van de belangrijkste theoretische inzichten en verbindt deze tot een coherente theorie. Onze theoretische beschouwing van vertrouwen is dan ook grotendeels gebaseerd op Hardins werk. Hardin behandelt zelf ook de andere zienswijzen van vertrouwen (zie Hardin 2006: 25, 32).

[278] Andere benaderingen focussen op de morele verplichting van de vertrouwde persoon of op diens psychologische kenmerken of karaktereigenschappen (zie Hardin 2006: 17).

persoon wordt verwacht dat hij in de toekomst die belangen behartigt als waren het zijn eigen belangen. Hieruit volgen drie kenmerken die wij in afzonderlijke secties beschouwen, te weten (kenmerk A) de driehoeksrelatie (sectie 8.4), (kenmerk B) een reden voor vertrouwen (*incentive*, sectie 8.5) en (kenmerk C) een risico (sectie 8.6).[279]

A: Driehoeksrelatie

Allereerst is vertrouwen volgens Hardin een soort driehoeksrelatie: A vertrouwt B met betrekking tot x (Hardin 2006: 19). Om te begrijpen hoe vertrouwen in het sociale verkeer werkt, moeten allereerst deze drie elementen (A, B en x) duidelijk zijn. In het kader van deze studie is A de veiligheidsdienst, B de CIE/RIO en x operationele informatie met betrekking tot terrorisme. Bij het analyseren van deze drie elementen van vertrouwen is met name de machtsverhouding tussen A en B van groot belang. Indien A hiërarchisch boven B staat, is vertrouwen voor A niet echt noodzakelijk om het eigen belang door B behartigd te zien worden: dwang is voor A immers ook een optie. En A hoeft niet bang te zijn voor een (sociale) sanctie door B op het moment dat hij het vertrouwen van B schendt. Andersom is het voor B ook moeilijk om A te vertrouwen omdat het minder waarschijnlijk is dat A zijn (B's) belangen boven de eigen belangen zou stellen. Het al dan niet bestaan van machtsverhoudingen speelt bij vertrouwen dus een belangrijke rol in die zin dat machtsverhoudingen vertrouwen minder van belang maken. Uit het bovenstaande volgt mijn inziens dan ook dat de formele machtspositie van minder belang is dan de materiële: zolang *beide* actoren over en weer in staat zijn om bijvoorbeeld de sociale relatie eenzijdig te verbreken indien het vertrouwen wordt geschonden, is er sprake van een zeker machtsevenwicht en speelt vertrouwen een belangrijke rol. Indien één van beide partijen dit niet kan, dan is er natuurlijk nog steeds sprake van een interactie tussen actoren, maar kunnen ook andere elementen dan vertrouwen een rol spelen, zoals dwang. Om te kunnen spreken van vertrouwen in sociale relaties is dan ook een zekere mate van wederkerigheid en gelijkwaardigheid nodig, waarbij beide partijen er belang bij dienen te hebben dat de relatie standhoudt.

B: Een reden voor vertrouwen (incentive)

Een tweede kenmerk van vertrouwen is dat er sprake is van een reden (een *incentive*) om een ander te vertrouwen en een sociale relatie aan te gaan. Mensen kunnen andermans belangen incorporeren in de eigen belangen omdat ze (vanwege uiteenlopende redenen) belang hechten aan het voortduren van de sociale relatie met die ander. Een andere mogelijke reden is dat de vertrouwde partij belang hecht aan de reputatie betrouwbaar te zijn. Het gaat hem dan niet zozeer om de concrete sociale relatie met de vertrouwer, maar veel meer om mogelijke toekomstige andere sociale relaties waarin vertrouwen een rol speelt (zie Hardin 2006: 19).

[279] Een vierde kenmerk zou mijn inziens de context van de sociale relatie moeten zijn. Een sociale context is een andere dan een organisatorische, en leidt tot een andere invulling van de door Hardin genoemde kenmerken van vertrouwen. Zie ook: Kramer (2001: 168). Hardin noemt overigens wel het vergelijkbare verschil tussen sociaal kapitaal en organisatie kapitaal, en stelt dat de laatste in bepaalde gevallen interactie tussen actoren mogelijk maakt zonder dat er sprake is van vertrouwen (Hardin 2006: 79).

C: Risico

Het derde relevante kenmerk van vertrouwen is dat van risico: er is altijd een kans dat het vertrouwen niet gerechtvaardigd blijkt te zijn. Mogelijk plaatst A zijn eigen belangen (of die van anderen) boven die van B en wordt het vertrouwen van de laatste geschonden. Hoe groot een dergelijk risico is, hangt af van zowel de ernst als de waarschijnlijkheid van het schenden van vertrouwen.[280] In sommige gevallen is de waarschijnlijkheid dat iemand het vertrouwen schendt zeer klein, maar zijn de gevolgen ervan niet te overzien en dat maakt het totale risico dan te groot. En andersom zal een zeer hoge mate van waarschijnlijkheid dat het vertrouwen wordt geschonden met betrekking tot een minder ernstige zaak eveneens leiden tot een te groot risico. Uit deze kenmerken van risico (en dan met name de component van waarschijnlijkheid) volgt dat vertrouwen in dezelfde cognitieve categorie als kennis valt. Vertrouwen is immers afhankelijk van de kennis van de vertrouwende partij over de betrouwbaarheid van de andere partij (zie Hardin 2006: 17-18). In dit opzicht kan men ook niet kiezen om iemand te vertrouwen, maar de mate van vertrouwen is afhankelijk van de mate van kennis omtrent die ander.[281] Indien iemand het vertrouwen schendt, dan is het ongerechtvaardigde vertrouwen te wijten aan gebrekkige kennis omtrent die andere persoon. Omdat vertrouwen cognitief is en direct te relateren is aan kennis, speelt 'bekendheid' tussen de partijen een grote rol: de mensen met wie je goed bekend bent, zoals familie en vrienden, zijn ook die mensen van wie je het beste kunt beoordelen of ze betrouwbaar zijn of niet (Hardin 2006: 39). Hoe minder je weet van anderen, des te minder goed je in staat bent om de betrouwbaarheid in te schatten.[282]

8.4 Kenmerk 1: de driehoeksrelatie

In deze sectie behandelen wij hoe de driehoeksrelatie tussen de AIVD en de CIE/RIO in de praktijk vorm krijgt. Voor het beschrijven van deze relatie is het van belang vanuit welk perspectief wordt geredeneerd. De AIVD zal doorgaans andere uitgangspunten hanteren dan de politie. Uiteindelijk streven beide organisaties een effectievere terrorismebestrijding na, maar over de wijze waarop dat dient te gebeuren lopen de meningen uiteen. Zo zal de AIVD met name een verbetering en handhaving van de eigen informatie- en inlichtingenpositie beogen en ziet hij zichzelf daarbij (begrijpelijk, gezien de traditionele positie van de AIVD) als de belangrijkste partij. Politiegegevens zijn voor de AIVD een middel om de eigen informatiepositie te verbeteren.

De CIE/RIO is vanzelfsprekend ook op zoek naar een verbetering van de eigen informatiepositie. Zij behoeft hiervoor echter niet direct informatie van de AIVD te krijgen. Uit ons onderzoek blijkt dat de medewerkers van de CIE/RIO met name meer gelijkwaardigheid ten opzichte van de AIVD wensen. In de woorden van een respondent:

---

[280] De formule van risico is: ernst * waarschijnlijkheid.

[281] De beschikbare relevante kennis omtrent de ander constitueert (of, minder stellig geformuleerd, is medebepalend voor de mate van) het vertrouwen (Hardin 2006: 17).

[282] Het is daarom niet verwonderlijk dat informatiestromen binnen politieorganisaties (en wellicht ook andere overheidsorganisaties) vaak via '*old boys networks*' gaan en niet via de officiële kanalen waarbij de andere partij vaak anoniem is. Deze informele netwerken gaan uit van vertrouwen en de leden van deze informele netwerken kennen elkaar. Dat maakt het risico om met de ander informatie te delen kleiner. Zie ook subsectie 7.6.4 voor een beschrijving van het *old boys network* bij de politie.

"*De AIVD moet zich meer bewust worden van de politieorganisatie. Ze moeten ons beter bij dingen betrekken. Niet zoals die situatie bij het Laakkwartier. Op het allerlaatste moment een AT* (Arrestatie Team, opmerking auteur) *inschakelen, als je later eens leest wat ze allemaal weten. Ik hoop dat ze daarvan hebben geleerd.*" Interview teamleider CIE (A), oktober 2008.

Gelijkwaardigheid behoeft niet per se getoond te worden door informatieverstrekking op basis van wederkerigheid, maar kan bijvoorbeeld ook door middel van meer tijdige ambtsberichten van de AIVD plaatsvinden. Overigens stelde de Commissie Havermans (2004) ook al dat de partners van de AIVD (zoals het OM en de politie) doorgaans negatief over de AIVD oordeelden en dat de AIVD zich volgens de partners beter bewust moest worden van zijn rol in de bredere veiligheidsketen. Dit is dus niet alleen een wens van de politie in het algemeen en de CIE/RIO in het bijzonder.

Het perspectief van waaruit zaken als interactie en reciprociteit worden bekeken is dus van groot belang voor de beoordeling of de onderlinge interactie goed verloopt. Een overleg is voor de AIVD succesvol op het moment dat (1) de eigen informatiepositie is gehandhaafd, bijvoorbeeld doordat bepaalde politiële onderzoeken waarbij agenten van de dienst in beeld zijn gekomen zijn stopgezet, of (2) is verbeterd, bijvoorbeeld doordat de politiële onderzoeken informatie hebben opgeleverd die voor de AIVD van belang is en die kenbaar wordt gemaakt. Vanuit het oogpunt van de politie behoeft zo'n overleg echter niet direct succesvol te zijn geweest. Haar belangen kunnen immers ondergeschikt zijn gebleken aan die van de AIVD.

Omdat wij onderzoek hebben gedaan bij de politie, hebben wij met name inzicht in het politieperspectief. Voor het doen van objectieve uitspraken over de verhouding tussen de organisaties gebruiken wij het hierboven gegeven theoretische model van vertrouwen van Hardin. Aan de hand van dat model beoordelen wij of en, zo ja, in welke mate, er sprake is van het voor samenwerking noodzakelijke vertrouwen.

We beginnen deze sectie met het behandelen van de traditionele afstemming en communicatie tussen de diensten (subsectie 8.4.1). Vervolgens gaan we in op de wijze waarop de formeel juridische hiërarchische verhouding in de praktijk uitwerkt (subsectie 8.4.2). Daarna behandelen we de feitelijke informatie-uitwisseling tussen de politie en de AIVD in de praktijk (subsectie 8.4.3). We besluiten met een algemene sectieconclusie (subsectie 8.4.4).

8.4.1 Traditionele afstemming en communicatie

De afstemming en communicatie tussen de AIVD en de politie zijn van oudsher problematisch (zie Havermans 2004; Hoekstra 2004: 113-123). Dit geven verschillende respondenten ook zo aan. Een voorbeeld ter illustratie volgt hieronder.

"*Er is jaren bijna geen communicatie geweest. Waarom dit was? De AIVD wilde dat niet. Die roepen direct 'bronnenbescherming' en weigeren dan te communiceren. Natuurlijk vormt de wetgeving een barrière tegen samenwerking: omdat wij transparant moeten zijn en alles tegenover een rechter moeten verantwoorden, zal de AIVD niet snel met ons samenwerken. Maar naast deze wettelijke barrière is er ook nog een barrière op het menselijk vlak. Het gaat om hoe de AIVD naar ons kijkt. Dit*

is een vermoeden van mij, zeker weet ik het niet. Maar ik krijg het idee dat ze denken alles beter te weten dan de politie. Hautain." Interview runner CIE (B), oktober 2008.

Inderdaad, zoals in subsectie 8.4.2 nog zal worden betoogd zijn het in zekere zin concurrerende organisaties. Dit bemoeilijkt een open houding en communicatie. Daarnaast wordt de informatie-uitwisseling (een essentieel element van communicatie) in verregaande mate gereguleerd. Ook dit staat een effectieve en efficiënte communicatie doorgaans in de weg. We zullen overigens niet diep ingaan op de juridische aspecten van deze afstemming: dat is al in hoofdstuk vier besproken. We vervolgen deze sectie met een behandeling in 8.4.2 van de mogelijke hiërarchische verhouding tussen de AIVD en de CIE.

8.4.2 Een hiërarchische verhouding

In deze subsectie staan wij stil bij de wijze waarop de afstemming in de praktijk doorgaans plaatsvindt en hoe er wordt gecommuniceerd. Daarnaast behandelen wij in deze sectie ook de beeldvorming die het gevolg is van de door ons geschetste afstemming.

De verhouding tussen de AIVD en de CIE/RIO kan worden gezien als een hiërarchische verhouding. Allereerst wordt de verhouding bepaald door de strikte organisatorische en juridische scheiding tussen de AIVD en de politie. Artikel 9 van de WIV 2002 houdt in dat de medewerkers van de AIVD geen opsporingshandelingen mogen verrichten. Vanuit de veiligheidsdienst bezien is het dus duidelijk: geen opsporing door de dienst. Hoewel het in het licht van een democratische rechtsstaat wenselijk is om hoge- en lage politiediensten van elkaar te scheiden, wijst de praktijk uit dat er wel veel raakvlakken zijn. Het is immers goed denkbaar dat de politie tijdens een opsporingsonderzoek op informatie stuit die van belang kan zijn voor de AIVD, en andersom kan de AIVD ook op informatie met betrekking tot strafbare feiten stuiten die weer voor de politie van belang kan zijn. Zoals we hiervoor hebben betoogd, wordt dit alleen maar meer naarmate de organisaties meer op elkaar gaan lijken en op dezelfde aandachtsgebieden actief worden. Hieraan probeert de wetgever tegemoet te komen door mogelijkheden te creëren voor onderlinge informatie-uitwisseling. Zo kent de WIV 2002 een specifieke procedure voor informatieverstrekking door de AIVD aan onder meer de politie en het OM: de procedure van de ambtsberichten (artikel 38 WIV 2002).

Voor het beoordelen van een mogelijke hiërarchische relatie tussen AIVD en CIE/RIO is het ook van belang te beseffen dat de procedure van het ambtsbericht een discretionaire bevoegdheid is van de dienst: de AIVD is niet verplicht om de politie of het OM informatie te verstrekken (zie Van der Bel et al. 2009; zie ook subsectie 3.4.2). Het zou de goede taakuitvoering van de dienst immers niet ten goede komen als van ieder strafbaar feit melding gemaakt zou moeten worden. Overigens merkt de wetgever hierbij op dat de discretionaire ruimte minder wordt naarmate het strafbare feit ernstiger is (zie ook subsectie 3.4.2). De AIVD heeft dus veel ruimte bij het al dan niet verstrekken van informatie aan de politie. Dit geldt geenszins voor verstrekkingen van de politie aan de AIVD: de politie heeft een verplichting om informatie te verstrekken die voor de AIVD van belang kan zijn. Dit wordt ook in artikel 60 tot en met 62 WIV 2002 geregeld.

Politieambtenaren kunnen tijdens het werk in aanraking komen met informatie die van belang kan zijn voor de bescherming van de nationale veiligheid. Ook hierin voorziet de WIV 2002 in een verstrekkingsmogelijkheid. Artikelen 61 en 62 WIV

verplichten onder meer de ambtenaren van de politie (en dus ook medewerkers van de CIE/RIO) om (1) te beoordelen of informatie relevant kan zijn voor de dienst en, (2) zo ja, deze te verstrekken.[283] Het gaat hier om een verplichting. Dit is een belangrijke aanwijzing voor de aard van de verhouding tussen de CIE/RIO en de AIVD en heeft consequenties voor de rol van vertrouwen: de dienst heeft de bevoegdheid informatie aan de politie te verstrekken, terwijl de politie de verplichting heeft. Hieruit volgt in ieder geval dat de wetgever een bepaalde functionele hiërarchie aanbrengt tussen de organisaties, waarbij de bescherming van de nationale veiligheid van groter belang wordt geacht dan de bestrijding van criminaliteit. Van een wederkerige relatie tussen de organisaties is in dit opzicht dus geen sprake.

"*Vertrouwen ja, maar wederkerigheid nee. Wij zijn anders, wij zijn geen regiokorps. Dat er geen wederkerigheid is, volgt ook uit de wet: de politie is verplicht informatie die voor de AIVD van belang is aan de dienst te verstrekken, wij zijn bevoegd. Wij kunnen ook niet wederkerig zijn, er is een scheiding tussen de bevoegdheden van de dienst en van de politie.*" Interview (voormalig) medewerker AIVD (A), januari 2008.

Het feit dat er geen sprake is van wederkerigheid tussen de organisaties, heeft belangrijke gevolgen voor de onderlinge verhouding en voor de beeldvorming. Verschillende respondenten geven aan dat de AIVD zich in hun ogen superieur acht aan de politie. In de woorden van een respondent die tijdens het interview werkzaam was bij de politie maar voorheen bij de AIVD heeft gewerkt:

"*Ze vinden zichzelf ook heel belangrijk. Ons als politie hebben ze wat minder hoog zitten. Ze zouden ons meer kunnen vertrouwen. Ze maken ons artikel 60 ambtenaar met alles wat daarbij komt kijken, wij hebben ook die sterke geheimhoudingsplicht (…). Maar echt vertrouwen doen ze je niet. Ik kreeg het gevoel dat de medewerkers van de dienst het lastig vinden om met externen te praten, ook al zijn het artikel 60 ambtenaren.*" Interview (voormalig) medewerker AIVD (C), februari 2008.

Volgens de respondenten is er vanuit de AIVD te weinig oog voor de belangen van de politie, en wordt de politie veel meer gezien als één van de hulpmiddelen van de dienst in plaats van een volwaardige (gespreks)partner. Dat de dienst geen besef heeft van de taak en de mogelijkheden van de politie, wordt overigens ook door een respondent die werkzaam is bij de AIVD bevestigd. In enkele gevallen klinkt er bewondering door bij de respondenten voor de manier waarop AIVD-ers in het werk staan. Ze zijn over het algemeen hoger opgeleid en denken vaak wat verder vooruit voordat ze handelen, iets wat politiemensen doorgaans weinig doen. Uit zowel de interviews als de observaties blijkt dat AIVD-ers goed voorbereid bij vergaderingen en overleggen aanwezig zijn, dit in tegenstelling tot de politie.

"*AIVD-ers zijn meesters in manipulatie van politiek (…). Ik heb ze gesprekken met de politiek zien voorbereiden, dan gaan ze echt bij elkaar zitten en spreken ze af wat ze eruit willen halen, hoe ze dat bereiken etc. Dat gebruiken ze en volgens mij misbruiken ze dat ook. (…) Ze zitten vaak tot 's avonds laat voor te bereiden. (…) Hier zit ook een groot verschil met de politie. Wij bereiden bijna niks voor. Het is*

[283] Een dergelijke relevantie wordt geacht aanwezig te zijn indien de informatie past binnen de taakstelling van de AIVD. Artikel 61 WIV 2002 regelt de verplichting van de OM, artikel 62 WIV 2002 de verplichting van de politie. Formeel dient de verstrekking van deze gegevens door de politie eerst aan een 'artikel 60 ambtenaar' plaats te vinden.

eigenlijk soms beschamend. Kijk, politiemensen zijn doeners, pragmatisch. Maar dat betekent vaak ook dat ze een vergadering waar echt belangrijke zaken worden besproken niet voorbereiden. Ik heb onze leidinggevenden tijdens een vergadering nog even snel stukken door zien lezen. Die vergadering was al begonnen. Dan heb je het eigenlijk al verloren." Interview (voormalig) medewerker AIVD (D), juni 2009.

De WIV 2002 en andere relevante wetgeving zijn in dit opzicht zogenoemde 'juridische ordeningsprincipes' en hebben tot doel om sociale interactie mogelijk te maken in die gevallen waarin er geen sprake is van vertrouwen. De WIV 2002 doet dat door een hiërarchie aan te brengen tussen de organisaties. Vertrouwen lijkt daarmee niet meer noodzakelijk voor de 'samenwerking' (zie Hardin 2006: 107). Het is echter nog maar de vraag of een juridisch ordeningsprincipe het wint van andere (sociale) ordeningsprincipes. Kan de naleving van de wet bijvoorbeeld effectief worden afgedwongen? Met andere woorden: is de formeel juridische verhouding gelijk aan de materiële verhouding in de praktijk? Het antwoord op deze vraag luidt onzes inziens 'nee', voor zover wij van die praktijk kennis hebben genomen.

De hiërarchie tussen de AIVD en de CIE/RIO zorgt voor een hele sterke sociale categorisatie en een proces van *ingroup* en *outgroup* vorming (zie subsectie 7.5.3 voor de relevante sociaal psychologische theorie). Beide organisaties hebben een sterke eigen identiteit en beschouwen de andere organisatie als afwijkend en schrijven de ander negatieve kenmerken toe (dit hebben we overigens met name bij de CIE/RIO kunnen vaststellen en minder bij de AIVD). Deze vaststelling heeft weer gevolgen voor de wijze waarop de organisaties communiceren en informatie uitwisselen, zie subsectie 8.4.3.Wij zullen de wijze waarop de relatie vormt krijgt en de verschillende modaliteiten van interactie eerder behandelen in sectie 8.9.

8.5 Kenmerk 2: De reden voor vertrouwen (*incentive*)

In sectie 8.2 hebben wij de vermindering in de verschillen tussen de organisaties behandeld en hebben wij al gesteld dat de organisaties steeds meer de activiteiten moeten afstemmen en moeten gaan samenwerken. Zo stelde de commissie Havermans in 2004 "*de Commissie constateert dat de AIVD soms over voor het strafproces relevante informatie beschikt en constateert eveneens dat in de justitieketen de gedachte sterker gaat leven dat het op grond van intelligence voorkomen van strafbare feiten ook tot de taak van politie en justitie behoort.*" (Havermans 2004: 104-105). Volgens de Commissie Havermans vervaagt het klassieke onderscheid tussen de activiteiten van de AIVD en de CIE, hetgeen problemen oplevert met betrekking tot operationele planning en bestuurlijke verantwoordelijkheid (Havermans 2004: 107). Vanwege de in sectie 8.2 beschreven ontwikkelingen bij de politie kan de politie nu in een fase optreden die voorheen was voorbehouden aan de AIVD. De kans dat agenten en informanten van de AIVD zich schuldig maken aan strafbare feiten en daarmee het doelwit worden van politieoptreden is tegenwoordig dan ook veel groter dan vroeger. Een respondent verwoordt dit als volgt.

" (…) *Met het naar voren trekken van het strafrechtelijke verdenkingscriterium en de strafbare voorbereidingshandeling krijg je wel dat agenten sneller strafbaar betrokken zijn bij strafbare feiten. Bijvoorbeeld bij het voorbereiden van terroristische aanslagen: het is in principe al voldoende om bij het bespreken van een aanslag aanwezig te zijn.*" Interview (voormalig) medewerker AIVD (A), januari 2008.

De AIVD wil dat zijn agenten en informanten zo dicht op terroristische organisaties zitten als mogelijk, en vaak betekent dit dat zij er ook deel van uit maken. Dit maakt het zeer waarschijnlijk dat ze in beeld komen van de politie, hetgeen de AIVD koste wat het kost wil voorkomen.[284] Dit betekent dat de AIVD operationele redenen heeft om met de politie samen te werken.

De AIVD en de CIE/RIO hebben bij deze stand van zaken voldoende redenen om de sociale relatie in stand te houden en elkaar te vertrouwen. Naast de operationele noodzaak en het streven naar zoveel mogelijk informatie is er ook sprake van politieke druk om samen te werken. We vervolgen met een illustratief citaat.

"Er zitten aan dat naar voren schuiven van het strafrecht natuurlijk voordelen en nadelen. Als strafrechtelijk optreden eerder mogelijk is, dan kan de politie gemakkelijk een zaak opbouwen, maar voor de dienst kan dat betekenen dat je eerder stopt. Andersom, als strafrechtelijk optreden later mogelijk is, dan is er voor de dienst veel mogelijk en kunnen wij langer doorwerken, maar voor de politie is het lastig omdat ze dan pas laat kunnen optreden. Om in deze problematiek te voorzien is er een periodiek afstemmingsoverleg. Voor een goede samenwerking is vertrouwen en acceptatie nodig." Interview (voormalig) medewerker AIVD, januari 2008.

Nu beide organisaties belang hebben bij samenwerking en de juiste drijfveer hebben om elkaar te vertrouwen, lijkt het voor de hand te liggen dat de organisaties ook daadwerkelijk samenwerken en elkaar vertrouwen. Toch blijkt keer op keer dat het vertrouwen niet vanzelfsprekend is. In het veld wijst men vaak naar cultuurverschillen en de strijd om de budgetten als onderliggende oorzaken van ontbrekend vertrouwen. Ook de Commissie Havermans (2004: 100) stelt dat er vóór 2004 redelijk wat weerstand was bij zowel de AIVD als de CIE/RIO om informatie met elkaar te delen, en wijt dit aan grote cultuurverschillen. Zoals hierboven reeds is betoogd, kan er in een dergelijke hiërarchische machtsverhouding nauwelijks sprake zijn van vertrouwen, hetgeen de interactie tussen de organisaties niet ten goede komt.

8.6 Kenmerk 3: Risico

Nauw verbonden met vertrouwen is geheimhouding. Geheimhouding hebben we al eerder in sectie 2.6 behandeld. Hier behandelen we de geheimhouding voor zover relevant voor de vertrouwensrelatie tussen de AIVD en de CIE/RIO: het inter-organistorische perspectief op geheimhouding (zie subsectie 2.6.1). Volgens Simmel is geheimhouding essentieel voor de relatie tussen mensen en groepen: "*iedere relatie tussen twee individuen of twee groepen wordt gekenmerkt door de hoeveelheid geheimhouding die erbij betrokken is*" (Simmel 1906: 21). Vertrouwen is een hypothese omtrent toekomstig gedrag en daarmee zweeft het volgens Simmel tussen volledige kennis omtrent de ander en een volledig gebrek aan die kennis: "*het beschikken over volledige kennis maakt vertrouwen niet langer noodzakelijk, en complete afwezigheid van kennis maakt vertrouwen duidelijk onmogelijk*" (Simmel

[284] De bronafscherming is voor de AIVD immers bijna 'heilig', zie sectie 3.3. Daarnaast betekent een eventuele aanhouding van een agent of informant van de AIVD dat de laatste een kostbare inlichtingenpositie kwijtraakt, hetgeen verregaande gevolgen kan hebben voor de operationele belangen van de AIVD.

1906: 13).[285] Of je iemand vertrouwt, hangt dus af van de kennis die je hebt omtrent die ander. Dit betekent dat een zekere transparantie van beide partijen nodig is om de relevante kennis ten behoeve van de betrouwbaarheid te verkrijgen. Hier zit volgens ons het grote probleem bij het vertrouwen tussen veiligheidsdiensten en de politie in het algemeen en de AIVD en de CIE/RIO in het bijzonder. Niet transparantie, maar geheimhouding is een essentieel aspect van de relatie tussen deze diensten.[286] De eersten worden niet voor niets ook wel 'geheime diensten' genoemd. Omdat je niet weet wat een geheime dienst precies met 'jouw' informatie gaat doen, kun je niet goed inschatten of, en zo ja, in hoeverre die dienst te vertrouwen is. Dit speelt een belangrijke rol in de relatie tussen de AIVD en de politie.

De AIVD heeft zoals gezegd geheimhouding hoog in het vaandel staan, maar hierin zijn ze volgens de politie doorgeslagen.

"*(…) AIVD en de RID zijn nogal makkelijk met het stempeltje confidentieel. Maar ik heb zelf vaak meegemaakt dat we uiteindelijk op een bepaalde manier toch aan die informatie kwamen. Wat bleek, het ging om informatie die je zo op het internet kunt vinden. Of erger nog, soms kregen wij een mutatie die oorspronkelijk van de politie was terug met daarop de stempel confidentieel/staatsgeheim.*" Interview runner CIE (B), oktober 2008.

De laatste situatie die door de bovenstaande respondent wordt aangegeven, staat bekend als de U-bocht constructie. Volgens sommige respondenten zou de AIVD meer kunnen delen dan ze op dit moment doet. Dit roept bij hen het beeld op dat de AIVD niet alleen legitieme operationele redenen heeft om informatie af te schermen, maar soms ook de eigen tekortkomingen probeert af te schermen.

"*Van de dienst zien we niet zoveel. Ze proberen altijd de informatie goed af te schermen. Met als gevolg dat je niet kunt aantonen waar de sterke en de zwakke punten van zo'n dienst liggen. Ik heb persoonlijk vaak de indruk dat zij onze informatie gebruiken om hun positie vast te stellen. Volgens mij is hun informatiepositie vaak schraal. Maar echt zeker weten doe je dit nooit. Het probleem is dat het een groot vierkant gebouw is waarvan je niet weet wat er precies in zit.*" Interview runner CIE (C), maart 2009.

Al met al is de geheimhouding die de AIVD ten opzichte van de CIE/RIO betracht vanuit het politie-perspectief problematisch. De geheimhouding van de AIVD geldt ook voor de verstrekker met betrekking tot zijn aan de dienst verstrekte gegevens: hij wordt niet op de hoogte gehouden van wat de dienst met de informatie doet. Dit maakt het voor een CIE/RIO heel moeilijk om de dienst te vertrouwen. Zij weet immers niet wat er uiteindelijk met de informatie gebeurt en kan dus niet inschatten of de dienst te vertrouwen is, dat wil zeggen: of de dienst de belangen van de CIE/RIO in de eigen belangen incorporeert. Het enige waar de CIE/RIO van uit kan gaan is de reputatie van de dienst als een geheime dienst, een dienst die de bron van informatie en de informatie zelf nooit onnodig prijs zal geven.[287] Maar of vervolgens de

[285] Simmel wijkt hiermee overigens af van Hardin: volgens Hardin is de mate van vertrouwen afhankelijk van de mate van kennis, en veel kennis betekent veel of weinig vertrouwen.
[286] Overigens merk ik hierbij op dat de AIVD wel wordt gecontroleerd. Zo is er een Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten en is er een parlementaire controle. Zie Commissie Havermans (2004: 77-104); CTIVD (2007) en Van der Bel et al. (2009: 197-201). .
[287] Zie voor het belang van reputatie bij vertrouwen Hardin (2006: 22-25).

belangen van de CIE/RIO worden behartigd, kan de CIE/RIO zelf niet of nauwelijks beoordelen.

Het delen van informatie brengt voor de CIE in abstracto teveel risico met zich mee. Een organisatie verliest door het delen van informatie invloed en autonomie, en deze concrete kosten wegen niet op tegen de abstracte baten (zo deze al aanwezig zouden zijn. Zie ook: Sales 2010; subsectie 2.3.2). Uit de antwoorden van de respondenten volgt dat zij het beeld hebben dat de AIVD met de politie-informatie "*aan de haal gaat*" (sociaal gesprek runner, januari 2011). Volgens CIE-ers ziet de AIVD de politie dus als een potentiële belangrijke bron voor informatie, en gebruikt de AIVD deze informatie in zijn adviezen en voor het (bij)sturen van de eigen inlichtingenoperaties, hetgeen volgens de respondenten niet zelden leidt tot het late stoppen van politiële onderzoeken. Met andere woorden: de invloed en de autonomie van de CIE/RIO en de politie in het algemeen hebben te lijden onder informatieverstrekking aan de AIVD. Het is daarom niet verwonderlijk dat medewerkers van de CIE/RIO (en politiemensen in het algemeen) huiverig zijn om informatie te verstrekken aan de AIVD.

Opvallend is dat vrijwel alle respondenten aangeven dat ze eigenlijk geen bewijs hebben voor bepaalde veronderstellingen, maar dat men met name een bepaald gevoel heeft. Het gaat hier dus om beeldvorming door politiemensen, waarbij de geheimhouding door de AIVD ruimte laat voor interpretatie. Hieruit volgt dat er sprake is van sterke sociale categorisatie (*ingroup/outgroup* vorming), waarbij aan de eigen organisatie positieve kenmerken worden verleend en aan de andere organisatie negatieve kenmerken.[288] Omdat de verstrekte informatie zeer summier is, gaan veel politiemensen over op het speculeren omtrent mogelijke achtergronden en motieven van de AIVD om informatie al dan niet te verstrekken. Deze dynamiek van geheimhouding hebben we in subsectie 7.6.1 ook al behandeld voor de interne situatie bij de politie. Hiervan lijkt ook sterk sprake te zijn bij de relatie tussen de AIVD en de CIE/RIO.

8.7 Conclusie: is er sprake van vertrouwen?

Met betrekking tot de driehoeksrelatie tussen de AIVD, de CIE/RIO en hetgeen waarover het vertrouwen zich uitstrekt kunnen we concluderen dat er formeel juridisch sprake is van een zekere mate van functionele hiërarchie. In de praktijk blijkt de CIE/RIO echter in staat om de verplichtingen om informatie aan de dienst te verstrekken te omzeilen. Feitelijk is er dus niet echt sprake van een machtsverhouding, waarmee er voldoende ruimte bestaat voor onderling vertrouwen. Daarnaast is er ook sprake van een sterke *incentive* om elkaar te vertrouwen: er is een hoge maatschappelijke en politieke druk op de organisaties om samen te werken. Dit

[288] Het is overigens opvallend dat respondenten, wanneer ze gevraagd wordt naar de verschillen tussen de organisaties, de eigen organisatie kenmerken toeschrijft die ze juist bij een andere vraagstelling of in andere situaties afwezig achten. Een voorbeeld is de respondent die tijdens een interview op de vraag naar wat het verschil is tussen de CIE en de AIVD antwoordt dat de CIE veel verder doordenkt dan de AIVD, en veel meer doorvraagt. Dit zou volgens hem komen door de ervaring op straat (binnen de politie wordt vaak gesproken over '*streetwise vs bookwise*'). Dezelfde respondent geeft tijdens een koffiegesprek echter aan dat de politie niet goed is in doordenken op een langere termijn, en dat dit één van de redenen is waarom IGP niet goed zal slagen. We zijn in meerdere gevallen gestuit op dergelijke discrepanties in de stellingen van de respondenten, waarbij het verschil met name zit in het onderwerp waarover gesproken wordt. Afgezet tegen de AIVD beschikt de CIE/RIO volgens de respondenten kennelijk over andere competenties dan wanneer zij op zichzelf (dus zonder *outgroup*) wordt beoordeeld.

laatste wordt gecombineerd met een grote operationele noodzaak. Een derde element van vertrouwen, te weten risico, is een problematisch element dat een volledig vertrouwen in de weg staat. Naarmate het risico groter wordt ingeschat, wordt het vertrouwen minder. Op een gegeven moment werd het risico heel groot ingeschat en van vertrouwen was toen dus geen sprake meer. Het problematische van geheimhouding is dat het een potentiële vicieuze cirkel is: geheimhouding komt voort uit wantrouwen en wantrouwen komt weer voort uit geheimhouding. Geheimhouding en vertrouwen gaan niet goed samen, hetgeen belangrijke gevolgen heeft voor de samenwerking tussen veiligheidsdiensten en de CIE/RIO. Vertrouwen staat weer in relatie tot de mate van mogelijke interactie tussen twee partijen. Veel vertrouwen leidt tot meer en gemakkelijke interactie, maar weinig vertrouwen leidt tot weinig en moeizame interacties.

Wij hebben hiervoor al aangegeven dat van de AIVD en de politie wordt verwacht dat zij in het kader van terrorismebestrijding meer de interactie opzoeken. Dit is met name het geval sinds de aanslagen van 11 september 2001 en de aanslagen in Madrid in 2004. Het wordt nu tijd om deze interacties eens nader te bezien.

We beginnen met de behandeling van de RID (sectie 8.8). Deze satelietorganisatie van de AIVD zou immers een grote rol kunnen spelen in de communicatie tussen de AIVD en de CIE. Na de RID staan we stil bij de drie belangrijkste modaliteiten van interactie tussen de AIVD en de politie. Zo vindt er afstemmingsoverleg plaats tussen de AIVD en de politie waarbij de CIE een belangrijke rol speelt (sectie 8.9). De tweede modaliteit van interactie is de stelselmatige informatie-uitwisseling, waarbij met name de CIE/RIO informatie aan de AIVD verstrekt (sectie 8.10). De laatste, meest verregaande modaliteit van interactie is de samenwerking, zoals bij de CT-infobox (sectie 8.11).

8.8 De RID

Voordat wij de modaliteiten van interactie behandelen, staan wij eerst kort stil bij de bijzondere positie van de RID. De RID heeft een dubbele taak: zij richt zich zowel op het uitvoeren van de WIV (de AIVD-taak) als op de openbare orde taak. Voor de AIVD taak werkt de RID zoals gezegd onder aansturing en verantwoordelijkheid van de AIVD. Veel communicatie tussen de AIVD en de politie vindt plaats met tussenkomst van de RID. Zo zijn er regionale afspraken gemaakt dat de CIE bepaalde informatie aan de RID verstrekt, die deze vervolgens naar de AIVD stuurt. Wij merken op dat de RID eigenlijk AIVD is voor zover hij de WIV-taak uitvoert. Dat maakt dat de CIE dan met de AIVD communiceert. Andersom wordt communicatie van de RID met de CIE gereguleerd door de WIV. De RID is in dat opzicht gebonden aan dezelfde verstrekkingsregels als de AIVD. Dit betekent dan ook dat veel van onze bevindingen met betrekking tot de AIVD ook gelden voor de RID. De RID behoeft daarom eigenlijk geen aparte behandeling. Wij constateren in de praktijk echter toch een verschil tussen de RID en de AIVD. Bij de RID werken namelijk politiemensen, en volgens enkele respondenten communiceert dit makkelijker. De RID zou dus een rol kunnen spelen in de modaliteiten van interactie en beter met de politie kunnen communiceren omdat zij in de kern ook politiemensen zijn en in dat opzicht dezelfde taal spreken. In de woorden van een respondent.

"*(…) Directe communicatie gaat vaak via de RID-en. Tussen politiemensen en AIVD-ers is zelden een op een contact. Dat gaat allemaal via (…) de RID-en. Tussen RID-ers en politiemensen is het wat makkelijker communiceren. Dat zijn ook gewoon*

politiemensen. Maar vergeet niet: het zijn wel artikel 60 ambtenaren. Zij vallen eigenlijk rechtstreeks onder het hoofd van de AIVD." Interview (voormalig) medewerker AIVD (D), juni 2009.

Er zijn dus voordelen aan de communicatie tussen de RID en CIE-ers: het zijn beiden politiemensen, en die vertrouwen elkaar sneller. Toch wordt er door sommige respondenten ook gewezen op een gevaar met de RID-ers, waaruit duidelijk wordt dat het vertrouwen in de RID ook niet vanzelfsprekend is. Een respondent verwoordt het als volgt.

"*Met de RID hebben we (…) weinig contact, maar dat zijn ook weer meer de loopjongens van de AIVD.*" Interview runner CIE (B), oktober 2008.

Sommige respondenten geven aan dat ze liever direct met de AIVD contact hebben. In de woorden van een hoofd CIE.

"*Wat echt een wazig iets is, is de RID. Dat is een beetje een vreemde organisatie. Ik pleit ervoor die club op te heffen en bij de korpsen gewoon liaison-officers van de dienst neer te zetten die het contact onderhouden. Anders krijg je situaties als 'nou, ik geef deze informatie niet aan de dienst, maar ik heb toch ook een artikel 60 status.' Dat werkt niet, je hebt dan politiemensen die als vazallen van de dienst worden gebruikt.*" Interview hoofd CIE (C), april 2009.

Wij hebben tijdens onze interviews en sociale gesprekken een aantal keren vernomen dat de dubbele taakstelling voor de RID-ers nog weleens problematisch kan zijn. Wanneer ze in de rol van AIVD-er informatie moeten vragen aan politiecollega's, dan merken ze dat de communicatie opeens een stuk stroever wordt. Dit heeft met name te maken met het feit dat de RID-er op dat moment valt onder de beperkingen van de WIV. Hij wordt dus in de communicatie geremd vanwege zijn wettelijke geheimhoudingsplicht. Collega's met wie ze in andere gevallen goed communiceren, zien dit volgens de respondenten als een plotseling wantrouwen, en reageren hier dikwijls negatief op. Een respondent die zelf voor de AIVD en de RID heeft gewerkt, geeft overigens aan dat ondanks de periodieke communicatieproblemen de meeste RID-ers wel in staat zijn om de twee functies te combineren.

"*Ja, je hebt voortdurend twee petten in je hand. Maar op zich gaat dat switchen vanzelf, dat kost weinig moeite. In de praktijk heb je gewoon twee vakjes in je hoofd: dit is voor de AIVD en dit is voor de politie. De meeste medewerkers kunnen hier goed mee omgaan.*" Interview (voormalig) medewerker AIVD (D), juni 2009.

Wij sluiten deze sectie af met de opmerking dat wij weinig medewerkers van de RID hebben gesproken, en wij zullen daarom niet dieper op de rol van de RID ingaan. Daarnaast merken wij op dat bij terrorismebestrijding de RID doorgaans betrokken is vanuit de AIVD-rol.[289] In het kader van ons onderzoek beschouwen wij de RID en de AIVD dan ook als dezelfde organisatie en onze bevindingen zijn voor een groot deel voor beide organisaties hetzelfde. Wij vervolgen onze verslaglegging van het praktijkonderzoek met de behandeling van de drie modaliteiten van interactie.

[289] Een uitzondering is het onderzoek naar radicalisering. Dat vindt vaak plaats in het kader van de openbare orde taak.

8.9 Afstemming en overleg door middel van het AOT/IOT

De eerste modaliteit van interactie is de afstemming van activiteiten. Hiervoor is relatief weinig vertrouwen nodig, en dit is dan ook een modaliteit van interactie die in de praktijk vrij succesvol blijkt. Afstemming wordt gezocht tijdens de overlegvormen van het AOT (Afstemmingsoverleg Terrorisme) en het IOT (Inlichtingenoverleg Terrorisme). Het doel van overleg en afstemming is dat er in specifieke casus informatie (of kennis) wordt uitgewisseld dan wel overgedragen, maar dat de daaropvolgende activiteiten van de betrokken partijen onder eigen verantwoordelijkheid plaatsvinden. Hierdoor behouden beide partijen invloed en met name autonomie. Dit is een belangrijk verschil met de hierna te behandelen samenwerking in de CT-infobox.

Het doel van het AOT en het IOT is met name dat de activiteiten van de organisaties op elkaar worden afgestemd. Bij het AOT zit een afvaardiging van de politie (tactische opsporing, CIE en RIO), OM en de AIVD. Daar worden de lopende onderzoeken van de politie besproken, waarbij de AIVD de mogelijkheid heeft om aan te geven in welke gevallen de opsporingsonderzoeken de belangen van de AIVD raken. Op basis van dit 'inlichtingenbelang' kan dan worden besloten om bepaalde onderzoeken stop te zetten. Ook is het mogelijk dat de AIVD tijdens dit overleg aangeeft welke onderzoeken volgens hem nodig zijn. Overigens worden beslissingen over het al dan niet uitvoeren of stopzetten van opsporingsonderzoeken door het OM en de politie genomen, waarbij het primaat ligt bij het OM (dat is immers het bevoegd gezag met betrekking tot de opsporing, artikel 12 Politiewet 1993). Het is dus niet zo dat de AIVD bij machte is om 'de stekker uit onderzoeken te trekken', zoals vaak wordt vermoed. Een respondent verwoordt het als volgt.

"*Die beelden over 'het stoppen van zaken' worden steeds versterkt. De leider van de opsporing is natuurlijk het OM, en niet de AIVD. Er is niet voor niets een landelijke OvJ aangesteld. Die zien de bredere verbanden. En als er dan een zaak wordt stopgezet, dan gaat dat via het OM. Als die landelijke OvJ de overtuiging krijgt dat bepaalde opsporingshandelingen niet passen of niet zinnig zijn vanwege activiteiten van de dienst, dan wordt een zaak stopgezet. Je moet dat dan (als politie, opmerking auteur) accepteren.*" Interview (voormalig) medewerker AIVD (A), januari 2008.

Bij het AOT worden de lopende tactische (opsporings)onderzoeken besproken. Hier worden doorgaans geen CIE-inlichtingen besproken. Voor afstemming tussen de CIE en de AIVD is het IOT in leven geroepen.

"*We zitten tijdens zo'n overleg bij elkaar en in het IOT bespreken we bijvoorbeeld welke bronnen wij van plan zijn om aan te lopen. De AIVD kan dan reageren in de trant van "we vinden het eigenlijk niet zo handig als jullie je bron daar gaan aanlopen. Daar hebben wij een inlichtingenbelang". Ze zeggen nooit 'je mag dit of dat niet doen'. Die positie hebben ze niet, en dat weten ze ook wel. Maar ze geven wel duidelijk aan "handen af". Dat voelt weleens irritant. Maar op zich kan ik daar wel vrede mee hebben.*" Interview teamleider CIE (D), november 2009.

De bedoeling van het IOT is dat de CIE en de AIVD de operationele activiteiten afstemmen. Net als bij het AOT zijn de politie, het OM, en de AIVD hierbij vertegenwoordigd, zij het ditmaal in een veel kleinere bezetting. Van de politie zijn alleen CIE-ers aanwezig. Overigens gaat het doorgaans om de CIE van het KLPD,

alhoewel er de laatste jaren ook steeds vaker bepaalde regiokorpsen aansluiten. Bij het IOT geeft de CIE aan welke inlichtingentrajecten er lopen waarvan zij van mening zijn dat ze aan belangen van de AIVD raken. Indien er inderdaad sprake is van een inlichtingenbelang, kan worden besloten om bepaalde CIE-trajecten stop te zetten. Zo kan de CIE een aantal namen bespreken van mensen die zij van plan zijn aan te lopen. De AIVD geeft dan aan welke nog aan te lopen informanten volgens hen de moeite waard zijn om te benaderen en bij welke dat niet verstandig is. Het komt ook voor dat er tijdens dit overleg wordt besloten tot het overdragen van informanten van de CIE aan de AIVD. Andersom vindt veel minder vaak plaats, volgens enkele respondenten helemaal nooit. Dit brengt ons op de realiteit van de overlegvormen. Hoe komen ze in de praktijk tot uitwerking? Hieronder behandelen we (A) in hoeverre het AOT leidt tot effectieve informatie-uitwisseling en afstemming tussen de AIVD en de CIE en (B) in hoeverre het IOT leidt tot effectieve informatie-uitwisseling en afstemming tussen de AIVD en de CIE.

A: AOT: effectieve informatie-uitwisseling en afstemming?

Over de overlegvormen zijn de politiemensen voorzichtig positief. Het AOT wordt met name door de collega's van de RIO en de tactische opsporingsteams positief beoordeeld. De meeste aanwezigen zijn van mening dat het een waardevol overleg is, waar relevante inzichten worden besproken en, wanneer mogelijk, gedeeld. Over het AOT is men binnen de CIE echter iets minder goed te spreken dan over het IOT. Volgens verschillende respondenten die in het verleden betrokkenheid hebben gehad met het AOT is de politie tijdens dit overleg geen gelijkwaardige gesprekspartner. Volgens een respondent is het AOT alsof er "klemmen op je hersenen worden gezet en je wordt leeggezogen". Anderen geven aan dat de betrokken teamleiders eigenlijk door de dienst worden overhoord over het onderwerp terrorisme en de ontwikkelingen die zij al dan niet waarnemen.

"*In het begin was het meer een soort examen voor (…) de teamleider (van het onderzoeksteam). Die gingen dan vertellen wat er in de onderzoeken gebeurt, en dat was puur eenrichtingsverkeer. Dan kreeg je wat lastige vragen, en dan had de AIVD een keer een ambtsbericht ingestuurd en daar wilden ze dan dat op gewerkt werd, maar hier zit je weer met de stuurploeg en ja, daar gaat dan wat tijd overheen. Dat overleg moet wel een bepaalde zin hebben. Als je alleen maar gaat zeggen wat al in een ambtsbericht is verstrekt, dan heeft dat overleg geen zin. Dat leek wel zo in het begin: de politie ging de ontwikkelingen in de onderzoeken vertellen en dat was het. Dus die overlegstructuur van het AOT is continu in ontwikkeling geweest. Maar het is een andere opzet nu. Je merkt dat de AIVD nu ook wat meer informatie gaat geven.*" Interview teamleider CIE (E), november 2010.

Tijdens het AOT is er dus volgens de betrokken politiemedewerkers met name sprake van eenrichtingsverkeer (waar echter langzaamaan verandering in komt).[290] Vanuit de AIVD bezien is dit echter niet vreemd. De aanwezige politiemedewerkers zijn immers over het algemeen geen medewerkers van de CIE en hebben daarmee niet de bijzondere positie in het strafproces die de CIE wel heeft. De kans dat informatie van de AIVD in het strafdossier terecht komt is bij dit overleg nu eenmaal groter dan bij

[290] Dat het er inmiddels anders aan toe gaat en de AIVD meer lijkt te delen, wordt tijdens een informeel gesprek met een aantal medewerkers die bij dat overleg aanwezig zijn bevestigd.

het (nog te bespreken) IOT. De dienst kan daarom minder informatie verstrekken aan de politie. Dit maakt echter ook dat de AIVD minder goed in staat is om bepaalde zaken toe te lichten. Wanneer zij zich beroepen op een inlichtingenbelang en daarmee via het OM een bepaald opsporingsonderzoek stilleggen of bijsturen, dan is door de politiemensen niet in te schatten wat dat belang dan is en waarom dat belang prevaleert boven het belang van de politie. Hoe dat op de politiemensen overkomt, wordt door een respondent als volgt geformuleerd.

"*Persoonlijk denk ik weleens: 'wat doen jullie eigenlijk met dat inlichtingenbelang?' Sommige zaken worden in stand gehouden die kwalijk zijn, maar dat wordt gedaan met het oog op een 'inlichtingenbelang'. Dit is echter mijn persoonlijke idee. Je kunt natuurlijk nooit helemaal weten wat de dienst weet.*" Interview teamleider CIE (D), november 2009

Volgens sommige respondenten is de term 'inlichtingenbelang' verworden tot "een machtswoord dat te pas en te onpas wordt gebruikt". Het gebruik van het woord 'machtswoord' is een goede indicatie voor hoe de politie haar positie in dit overleg ziet: als ondergeschikt aan de AIVD. Dit roept vanuit de politie een tegenreactie op. Zo geeft een respondent aan dat de AIVD volgens hem het liefste de preweegdocumenten (zie subsectie 7.2.1) en lopende onderzoeken zou beoordelen en accorderen. Dit is volgens de betreffende respondent echter de verantwoordelijkheid van de politie. Overigens geven veel respondenten ook aan dat ze zakelijk en professioneel met deze situatie om kunnen gaan.

"*(…) Het is irritant. Eigenlijk wil je er tegenin gaan. Het voelt een beetje alsof je als een klein kind aan de kant wordt gezet. Maar één seconde later denk ik 'prima'. Dan ga je zakelijk weer verder.*" Interview teamleider CIE (D), november 2009.

B: IOT: effectieve informatie-uitwisseling en afstemming?

Over het IOT zijn de meeste respondenten positiever. Binnen het IOT hebben de politiemensen het gevoel dat er meer gelijkwaardigheid is tussen de politie en de AIVD dan in andere gevallen. In het begin was dit overigens helemaal niet het geval en moesten beide partijen erg aan elkaar wennen. Maar inmiddels is men over het algemeen gematigd positief over het IOT. De betrokken partijen zitten fysiek bij elkaar en overleggen over het onderwerp terrorisme, hetgeen leidt tot een toename van het onderlinge vertrouwen. Toch is er net als bij het AOT tijdens het IOT met name sprake van eenrichtingsverkeer, waarbij de CIE de onderwerpen (aanlooplijsten) aanlevert waarover wordt gesproken en de AIVD met name hierop reageert.

"Wij geven aan welke mensen we willen aanlopen, en de dienst zegt dan welke we beter niet kunnen aanlopen in verband met een inlichtingenbelang. Ze noemen echt alleen het inlichtingenbelang en geven nooit aan waaruit dat belang precies bestaat. Ze zeggen dus niet wie er informant van de dienst is. Soms vindt er wel een bronnenoverdracht plaats. Ook weleens vanuit de dienst naar ons toe. Ik heb het nog niet meegemaakt, maar ik weet wel dat wij bronnen runnen die in het verleden ook bron van de AIVD zijn geweest. De AIVD zegt pas wie hun bron is als ze er klaar mee zijn en wij ze mogen hebben. Maar verder is ook dit overleg vrij open. Er vindt wel

een zinvolle informatie-uitwisseling plaats waar ook wij wat aan hebben." Interview teamleider CIE (D), november 2009.

Volgens enkele respondenten zal de CIE niet alle onderwerpen die onder de noemer van ideologische misdrijven vallen in het IOT brengen. Het gaat om gevallen waarbij volgens de CIE een gemeenschappelijk onderzoek plaatsvindt of waar de AIVD evident een inlichtingenbelang heeft. Bij islamitisch terrorisme zal de CIE vrijwel altijd overgaan tot bespreking in het IOT. Er zijn echter ook onderwerpen die weliswaar vallen onder de noemer van ideologische misdrijven, maar waarbij veel meer sprake lijkt te zijn van traditionele georganiseerde criminaliteit. In die gevallen kan de CIE ervoor kiezen om het niet in te brengen in het IOT.

"(…) *ik zeg wel dat wij afstemmen wie wij aanlopen, maar dat gebeurt pas wanneer er een gemeenschappelijk onderzoek is. Hierbij is 'gemeenschappelijk' dat waar de politie een onderzoek heeft dat in het taakveld van hen ligt zeg maar. Maar als wij een onderzoek draaien op X, (…) dan gaan wij dat niet aanmelden bij hen.*" Interview teamleider CIE (E), november 2010.

De CIE heeft dus een zekere mate van vrijheid bij het vaststellen van welke onderwerpen besproken worden bij het IOT. Overigens merken wij hier op dat ook de CIE-officier van justitie een belangrijke rol heeft bij het vaststellen wat wel en wat niet in het IOT wordt besproken. Uiteindelijk heeft hij (samen met de landelijke terrorisme officier) het laatste woord over welke onderwerpen besproken dienen te worden.

Ondanks het gegeven dat de meeste respondenten overwegend positief zijn over het IOT wordt er ook enige kritiek geuit. Allereerst zijn de meeste respondenten van mening dat de CIE een ondergeschikte rol speelt ten opzichte van de AIVD. Daarnaast zijn sommige CIE-ers van mening dat het IOT te bureaucratisch is. We zullen beide punten van kritiek kort behandelen.

Dat de CIE ondergeschikt is aan de AIVD blijkt volgens een enkele respondent uit de wijze waarop de AIVD het overleg invult. Volgens hen is de AIVD met name op zoek naar nieuwe informanten en deze respondenten geven aan dat zij het vermoeden hebben dat de politie een soort 'voorselectie' voor de AIVD mag doen. Zij zien het overleg met name als een manier van de AIVD om de eigen informatiepositie verder uit te bouwen en in stand te houden.

"*Ik heb persoonlijk vaak de indruk dat zij onze informatie gebruiken om hun positie vast te stellen. (…) Soms vang je een glimp op. Bij (zaak x) bijvoorbeeld. Wij hebben x gedraaid, en de AIVD schrok. Zij hadden de zaak aan ons overgedragen en waren dus de regie kwijt. Ze schrokken over wat wij aan informatie hadden binnengehaald: ze waren gewoon verbaasd over onze bronnen en wat die bronnen ons allemaal vertelden. Ze willen dus ook vaak bronnen van ons hebben.*" Interview runner CIE (B), oktober 2008.

Het IOT dient volgens deze medewerkers met name de belangen van de AIVD, en niet die van de CIE. Andere respondenten geven aan dat dit met name in het begin het geval leek te zijn, en dat de AIVD nu veel opener is geworden. Dit komt volgens de respondenten omdat de CIE net als de AIVD een verregaande mate van geheimhouding kan betrachten. De AIVD hoeft dan ook niet bang te zijn dat informatie in een procesdossier terecht komt en daardoor op straat komt te liggen. Dit

maakt de communicatie met de CIE gemakkelijker dan met bijvoorbeeld de tactische opsporingsteams. Een enkele respondent geeft aan dat de AIVD nog meer doordrongen mag worden van het feit dat de CIE ook een inlichtingendienst is, en niet alleen maar een onderdeel van de politie.

"*(…) Binnen de politie worden wij gezien als de inlichtingeneenheid, als degene die de geheimen heeft, die de embargo informatie heeft. Niet omdat wij graag geheimzinnig doen, maar gewoon omdat dat zo is geregeld dat niet iedereen dat mag weten (…). Dan ga je naar de AIVD, die in het begin gewoon zeiden 'dat is de politie', maar ze vergeten dat wij ook een inlichtingeneenheid zijn en dat ze gerust een geheimpje met ons kunnen delen, als dat binnen de WIV zou passen. Dat mis ik eigenlijk nog veel te veel. In wezen zien zij ons als de politie. Ze denken dat als ze ons wat vertellen, dat iedereen dat ook weet. Maar dat is dus niet zo.*" Interview teamleider CIE (E), november 2010.

Een bijzonder probleem ten aanzien van het IOT speelt intern bij de politie. Volgens sommige respondenten was er een beweging bij de AIVD om nog meer wederkerigheid in te brengen tijdens het IOT en daar ook verder te gaan in de informatie-uitwisseling dan men tot dan toe gewoon was (hoe ver en waarover het precies ging, konden de respondenten niet zeggen). Dit zou echter in zeer klein comité plaatsvinden: een teamleider van de AIVD, de directeur democratische rechtsorde, de CIE-officier van justitie, het hoofd CIE, het plaatsvervangend hoofd CIE en de landelijke officier van justitie inzake terrorismebestrijding zouden aanwezig zijn. Binnen de politie was men echter van mening dat in bepaalde gevallen ook andere politieambtenaren dan het hoofd CIE en diens plaatsvervanger bij het overleg aanwezig moesten zijn. Omdat deze medewerkers niet binnen de CIE werkzaam zijn, achtte de dienst het risico te groot dat AIVD-informatie breder werd gebruikt dan gewenst was. De AIVD heeft laten weten dat deze overlegvorm alleen met de CIE kan plaatsvinden en niet met andere politiële organisatieonderdelen. Dit is volgens diverse respondenten overigens een terugkerende discussie die de daadwerkelijke afstemmingsoverleggen tussen de AIVD en de politie in het algemeen vaak bemoeilijkt.

Al met al stellen wij vast dat onderlinge afstemming tussen de AIVD en de CIE in de praktijk door middel van het AOT en IOT succesvol lijkt te zijn. Dit is niet verwonderlijk, omdat hiervoor minder vertrouwen is vereist dan voor de verdergaande modaliteiten van interactie. Een stap verder dan afstemming gaat de stelselmatige informatie-uitwisseling. Deze behandelen wij in de volgende sectie.

8.10 Stelselmatige informatie-uitwisseling

Er zijn altijd situaties waarin de AIVD en de politie informatie moeten uitwisselen en moeten communiceren. In de meeste gevallen komt het erop neer dat de politie informatie heeft die van belang kan zijn voor de goede taakuitvoering door de dienst, en deze informatie moet worden verstrekt (artikel 62 WIV 2002). Daarnaast kan de dienst in situaties terecht komen waarin direct ingrijpen noodzakelijk is, zoals aanhoudingen wanneer er mogelijk sprake is van een op handen zijnde aanslag. Dit kan de dienst niet zelf, maar daarvoor moet de politie worden ingeschakeld. In subsecties 3.4.2 en 4.6.3 hebben we de juridische aspecten van verstrekkingen tussen de politie en de AIVD onderling al besproken. In deze subsectie behandelen we de wijze waarop dit in de praktijk gestalte krijgt. We behandelen (A) de

informatieverstrekking door de AIVD aan de politie, en daarna (B) de informatieverstrekking van de politie aan de AIVD.

A: Verstrekkingen door de AIVD aan de politie

De AIVD hecht in de praktijk bijzonder veel waarde aan de geheimhouding en schermt daarom zijn informatiepositie, bronnen en methoden af voor de buitenwereld, inclusief de politie. Wanneer de AIVD informatie heeft die voor de politie van belang is, wordt er een ambtsbericht verstrekt. Andere vormen van communicatie zijn doorgaans niet mogelijk: de WIV 2002 schrijft voor verstrekkingen aan de politie de procedure van het ambtsbericht voor (zie ook subsectie 3.4.2). In de ambtsberichten staat alleen die informatie die geen afbreuk doet aan de genoemde af te schermen belangen, hetgeen ze summier maakt. Daarnaast gaat er bijzonder veel tijd overheen voordat een ambtsbericht is opgesteld en goedgekeurd door de juridische afdeling van de AIVD. Volgens politiemensen maakt dit de communicatie van de dienst met de politie langzaam en inefficiënt. En als er uiteindelijk een ambtsbericht komt, dan is de inhoud beperkt en is de politie op zichzelf aangewezen om op zoek te gaan naar informatie.

"(Het) *kan heel lang duren, er moeten echt juristen naar kijken van kan dit zo. Kijk, als ze informatie hebben van over een uur ontploft daar en daar een bom of zo, dan denk ik niet dat dat zo gaat. Maar als het echt uitstel gedoogt, dan gaan er mensen naar kijken (…). Ik denk dat ze dan ook de bronnen van de informatie checken en kijken of dat kan (…). En goed, als juristen er naar gaan kijken, en dat weet jij nog beter dan ik, die gaan ieder woordje op een schaaltje wegen.*" Interview teamleider CIE (E), november 2010.

Ook bestaat er bij sommige respondenten het idee dat de AIVD opzettelijk informatie achterhoudt totdat het niet langer kan. Dit zouden zij doen om de eigen informatiepositie niet in gevaar te brengen. Immers, als de AIVD een ambtsbericht uitgeeft, verliest de dienst daarmee de controle over het traject. Het gevolg is echter dat de politie de informatie pas op een heel laat moment krijgt, waardoor er eigenlijk geen tijd meer is om een goed opsporingsonderzoek uit te voeren. Dit is volgens veel respondenten de belangrijkste reden waarom de opsporingsonderzoeken naar terrorisme doorgaans weinig succesvol zijn.

"*De spanning ligt met name op het moment waarop informatie wordt gedeeld. De dienst wacht zo lang mogelijk met een ambtsbericht versturen. Een voorbeeld; stel er is bij de dienst een Haagse groep in beeld. De dienst heeft daar al weken taps op draaien. Op een gegeven moment moeten wij als politie optreden. Wat je dan krijgt, is dat je een dag van tevoren de informatie pas krijgt. Dan heb je een paar uur om bewijs te verzamelen. Een veroordeling is dan niet mogelijk. Deze discussie loopt nog steeds. Ik heb niet de indruk dat we ver komen. Het is een lastige discussie.*" Interview hoofd CIE (C), april 2009.

Voor de politie is de informatie in een ambtsbericht vaak net voldoende om een opsporingsonderzoek op te starten of een lopend opsporingsonderzoek (enigszins) bij te sturen. Dit heeft natuurlijk waarde voor de opsporingspraktijk, maar de achterliggende informatie die bij de dienst blijft, is voor de politie onbereikbaar. Wat de verstrekte informatie dus feitelijk bewerkstelligt, is dat de politie meer capaciteit

kwijt is aan een zaak die 'van de andere kant van de schutting' komt.[291] Dit maakt ook dat men bij de politie over de inhoud en kwaliteit van de ambtsberichten niet echt te spreken is. Zoals wij hiervoor al hebben gesteld, bevatten de ambtsberichten weinig informatie. Enkele respondenten geven echter ook aan dat ze in sommige gevallen fouten bevatten of eenvoudigweg te weinig aanknopingspunten om een onderzoek op te starten.

"*Soms staat er in zo'n berichtje van een paar regels ook nog eens een fout. We hebben bijvoorbeeld een keer een onjuist IP-adres gehad. Dan krijg je zo'n klein berichtje, staat er alsnog een fout in."* Interview runner CIE (B), oktober 2008.

Wij hebben zelf tijdens ons onderzoek ambtsberichten gezien die in een terrorismeonderzoek waren verstrekt die alleen een naam van een subject bevatte, met daarbij de mededeling dat de betreffende persoon mogelijk betrokken is geweest bij het voorbereiden van terroristische aanslagen in het buitenland. In de praktijk is het overigens wel zo dat er sporadisch aanvullende ambtsberichten worden verstrekt, maar ook deze zijn zeer summier. Soms bevatten ze een telefoonnummer, soms een adres waar een subject zou verblijven. Volgens vrijwel alle respondenten die betrokken zijn bij onderzoeken naar terrorisme is dit veel te weinig. Overigens gaf één respondent aan dat een tactisch team dat is belast met onderzoeken naar terrorisme vaak meer ambtsberichten van de AIVD krijgt dan processen-verbaal van de CIE (interview teamleider RIO (C), april 2009). Dit zou met name te maken hebben met het feit dat het voor een CIE bijzonder moeilijk is om op terrorisme en gerelateerde onderwerpen een goede informatiepositie op te bouwen.

B: Verstrekkingen door de politie aan de AIVD

Zoals eerder gezegd is er een hiërarchische verhouding tussen de AIVD en de politie. Dit komt met name tot uitdrukking in de verstrekkingplicht van de politie. Op deze informatieverstrekking valt evenwel verder ook het één en ander aan te merken. De politie bepaalt namelijk zelf het moment waarop informatie wordt verstrekt, en volgens een aantal respondenten houdt de politie in bepaalde gevallen informatie extra lang achter.

"*(…) Wij bepalen zelf het tijdstip waarop de informatie naar de dienst gaat. En het gaat zeker niet weg zonder dat wij het beschouwen.*" Interview plaatsvervangend hoofd CIE, april 2009.

De oorzaak van het (langdurig) beschouwen is vooral gelegen in het feit dat het verstrekken van informatie aan de dienst kan betekenen dat bepaalde politieonderzoeken (CIE of tactisch) zullen worden stopgezet. Voor de politie is het onmogelijk om in te schatten wat er met de informatie gebeurt: de AIVD schermt

[291] Tijdens ons onderzoek hebben we twee van dergelijke gevallen geobserveerd. Met name bij terrorismezaken wordt weinig risico genomen en vindt een grote inzet van capaciteit plaats, zonder dat de politie van tevoren goed kan inschatten welke kant het onderzoek op zal gaan, of het eigenlijk wel resultaat oplevert of dat je na een paar weken intensief opsporen nog weinig bent opgeschoten. De formulering 'van de andere kant van de schutting' is in de politiepraktijk gebruikelijk voor het afschuiven van moeilijke zaken naar andere organisaties ('iets over de schutting flikkeren'). Volgens de commissie Havermans worden ambtsberichten door de politie en het OM onvoldoende opgevolgd (Commissie Havermans 2004: 107).

immers alle activiteiten af. Deze onzekerheid gecombineerd met de ervaring dat in bepaalde gevallen politieonderzoeken worden stopgezet, zorgt ervoor dat politiemensen terughoudend zijn met het verstrekken van informatie aan de AIVD en dat ze proberen het verstrekken van informatie zo lang mogelijk uit te stellen. Overigens is het aan de politie zelf om te beoordelen of bepaalde informatie van belang is voor de uitvoering van de AIVD-taak. Naast de termijn waarop wordt verstrekt, vinden er ook discussies plaats over welke informatie wordt verstrekt. Volgens diverse respondenten wil de AIVD altijd meer informatie van de politie, en is er voortdurend discussie over wat wel en wat niet door de politie wordt verstrekt. Er wordt door de meeste respondenten een onderscheid gemaakt tussen de tactisch bruikbare informatie met de code 01 en 11 (categorie één), en de 00, 200 en 300 informatie (categorie twee) die een verhoogd afbreukrisico kennen (zie subsectie 4.6.1). De eerste categorie wordt over het algemeen zonder problemen gedeeld met de AIVD, de tweede categorie is een voortdurend onderwerp van discussie. De AIVD is van mening dat ze die informatie ook moeten krijgen, en dat ze zonder enige vorm van controle toegang hebben tot deze categorieën informatie. De CIE stelt zich doorgaans op het standpunt dat deze informatie niet automatisch met de AIVD gedeeld mag worden. Je kunt immers geen afscherming van de identiteit van bronnen garanderen als de AIVD ongecontroleerd toegang heeft tot de informatie.

"*We kunnen moeilijk een bron beloven dat we zijn identiteit afschermen en zeggen "alleen de runners en het hoofd CIE zijn op de hoogte van het feit dat jij met ons praat… O ja, en ook nog 1500 anonieme AIVD-ers. Dat gaat niet.*" Interview hoofd CIE (B), februari 2009.

Het gaat volgens diverse CIE-ers niet zozeer om het gegeven dat de AIVD de beschikking krijgt over 00, 200 en 300 informatie, maar veel meer om het feit dat de AIVD de informatie wenst zonder dat de CIE weet over welke informatie het precies gaat. Ze raken hiermee de controle kwijt over waar welke informatie naartoe gaat, en dat levert weer mogelijke problemen op met de toekomstige inschatting van veiligheidsrisico's *et cetera*. Immers, als er een informant van de CIE wordt geliquideerd en er is mogelijk sprake van een lek, dan is het veel moeilijker voor de CIE (en andere politieorganisaties[292]) om te achterhalen waar het lek mogelijk zit. Het is dan ook volgens de CIE wenselijk dat er bij de CIE altijd zicht is op welke informatie naar de AIVD is gegaan.[293] Naast dit controleprobleem wijzen de CIE-en ook op het gevaar van het verliezen van de context waarbinnen de informatie is verzameld.

"*Het liefst kijken ze nog zonder login ofzo in zwacri (…). Dit vind ik geen goed plan. Het gevaar is namelijk dat ze direct in onze bestanden kijken zonder dat ze de context van de informatie weten of begrijpen. Het in zo'n bak kijken geeft geen context. Je kunt niet zien hoe groot een dreiging is, wat de impact is etc. Als wij iets tegenkomen voor de dienst, dan stel ik een verbaal op en geef ik het ze. Maar dan wel middels een verbaal, en het liefst met een gesprek zodat wij de informatie kunnen duiden.*" Interview teamleider CIE (A), oktober 2008.

[292] Dit soort zaken zal doorgaans bij de rijksrecherche belanden. Die beschikken overigens ook over een CIE.
[293] Dit wil de AIVD niet omdat het inzicht geeft in de informatiepositie van de dienst, en dit valt onder de geheimhoudingsplicht van artikel 15 WIV 2002.

Overigens maakt een enkele respondent een onderscheid tussen (1) 'basis-informatie' en (2) analyseproducten en strategische documenten, waarbij de eerste wel gedeeld kunnen worden en de tweede niet.

"*De AIVD kan dus zo inpluggen en al onze basisinformatie binnen trekken. Maar onze analyseproducten en strategische documenten, dat is een ander verhaal. Die hoeven wij niet te geven (…). Waarom? Ik wil daar zelf een keuze in hebben. Het is onze visie, onze interpretatie e.d. en daarover moeten wij zelf beslissen in hoeverre we die delen. Wij moeten daar ook zelf een uitleg over geven, dat helpt ook nog eens de communicatie.*" Interview hoofd CIE (C), april 2009.

Uit het bovenstaande blijkt dat de politie zoveel mogelijk controle probeert te houden over de verstrekking van informatie aan de AIVD. Ze willen het moment, de wijze en de inhoud van verstrekkingen in eigen hand houden. Daarnaast gaat het bij de bovenstaande vormen van informatie-uitwisseling om incidentgedreven (reactieve) informatie-uitwisseling: de CIE heeft informatie dat een persoon betrokken is bij terroristische activiteiten en verstrekt deze informatieop een zeker moment aan de AIVD. Dit is echter nog geen stelselmatige informatie-uitwisseling. De wetgever is van oordeel dat er wel sprake dient te zijn van stelselmatige informatie-uitwisseling, en heeft in de WPG getracht tot een oplossing te komen. Volgens artikel 24 WPG moet de dienst op basis van *hit- no hit* door de politiesystemen kunnen zoeken en indien er sprake is van een *hit*, dan moet de overeenkomende informatie onverwijld worden verstrekt aan de dienst. Hiermee verliest de politie de controle op het moment van de verstrekking en de beoordeling of bepaalde informatie van belang is voor een goede uitvoering van de taak van de AIVD. Op deze manier verstevigt de wetgever dus de hiërarchische verhouding tussen de AIVD en de politie, met als resultaat dat van vertrouwen minder snel sprake hoeft te zijn. Immers, de AIVD kan naleving van artikel 24 WPG afdwingen en de politie moet daar formeel juridisch gevolg aan geven. Zoals we hierboven hebben betoogd, is er in hiërarchische relaties weinig noodzaak tot vertrouwen.

Anno 2012 is er nog geen duidelijkheid over welke categorieën gegevens binnen het bereik van artikel 24 WPG vallen. De belangrijkste discussie vindt plaats omtrent de CIE-informatie, en het is goed mogelijk dat deze informatie wordt uitgezonderd van de werking van artikel 24 WPG. Maar zelfs al mocht dit niet het geval zijn en valt ook de CIE-informatie onder het bereik van artikel 24 WPG, dan betekent dit nog steeds niet dat de CIE geen mogelijkheden meer heeft om invloed op het verstrekkingproces uit te oefenen.[294] Zo geven diverse respondenten aan dat wanneer dit het geval is, de reactie van veel medewerkers van de CIE zal zijn om gegevens niet meer in de systemen in te voeren. Dit speelt ook al met betrekking tot de ontwikkeling naar *need to share* binnen de politie (zie subsectie 7.6.2), maar het zal volgens een aantal respondenten door de hier geschetste ontwikkeling verder worden aangejaagd. Als dit gebeurt, schieten ze het uiteindelijke doel van de stelselmatige informatie-uitwisseling voorbij met als gevolg dat er mogelijk minder relevante informatie aan de AIVD wordt verstrekt dan voordat artikel 24 WPG in werking trad.

[294] Zie voor de juridische ruimte van het OM om van deze juridische plicht af te wijken ook subsectie 4.6.3.

8.11 Samenwerking in het kader van de CT-infobox

De laatste modaliteit van interactie die wij behandelen is de samenwerking. Omdat dit het meeste vertrouwen vergt, is het in theorie de moeilijkste vorm. In de praktijk lijkt men echter door de oprichting van het samenwerkingsverband van de CT-infobox op het gebied van samenwerking verder te zijn gevorderd dan bij de afstemming en de stelselmatige informatie-uitwisseling.

De CT-infobox is de meest verregaande vorm van samenwerking tussen de politie en de AIVD. Na de aanslagen in Madrid in 2004 werd in Nederland de noodzaak gevoeld om de terrorismebestrijding een impuls te geven en effectiever te maken. Met name de versplintering van de verschillende actoren die bij de terrorismebestrijding zijn betrokken moest worden opgelost. Daarom werd direct na 'Madrid' de 'analytische cel' opgericht, een aanvankelijk kleinschalig samenwerkingsverband van AIVD, politie, en het OM met als doel ongeveer 150 personen die aan terrorisme konden worden gerelateerd 'onder controle te stellen' (Havermans 2004: 100; Van der Bel et al. 2009: 290). De analytische cel werd bij het KLPD ondergebracht, hetgeen de nodige problemen met betrekking tot de operationele samenwerking tot gevolg had.

De Commissie Havermans noemt als voorbeelden van de problemen (1) grote cultuurverschillen tussen de AIVD en de politie en (2) de weerstand bij beide partijen om informatie met elkaar te delen (Havermans 2004: 100). Het KLPD oordeelde volgens de commissie Havermans negatief over (1) de producten van de analytische cel, (2) de problematische samenwerkingsmogelijkheden en (3) de communicatie met de AIVD. De problemen kwamen deels voort uit de juridische complicaties. De WIV 2002 voorziet namelijk niet in een samenwerkingsverband zoals de analytische cel: artikel 15 WIV 2002 laat het delen van informatie met andere partijen op de manier bedoeld in de analytische cel eenvoudigweg niet toe. Men zocht naar kunstgrepen om toch binnen de box inhoudelijk te communiceren zonder dat informatie van de AIVD aan mensen die niet bij de AIVD werkten werd verstrekt.

"*We hadden afgesproken dat we bij die subjecten waar we volgens de dienst niets mee mochten een codewoord gebruikten: 'koffiemelk'. Dit was het codewoord voor 'handen af'. Dus soms vroeg je 'Karel, is subject .... misschien interress…? 'Koffiemelk!' Afblijven dus. Dit werkte in principe prima. Maar voor de politie was het wel lastig. Het werd wel begrepen, je kunt als dienst immers niet alles zomaar delen. De politie is niet dom. Maar je zou het soms weleens anders willen zien. Toen we naar Leidschendam gingen, was het codewoord niet meer nodig, omdat het KLPD net zo veel kon zien als iedere andere partij in de box.*" Interview (voormalig) medewerker AIVD, februari 2008.

Hieronder bespreken we (A) de oprichting van de CT-infobox, (B) de taken van de CT-infobox, (C) de interne werking van de CT-infobox, (D) de regionale CT-infoboxen en (E) de vraag of de CT-infobox daadwerkelijk kan worden gezien als een echt samenwerkingsverband.

A: De oprichting van de CT-infobox

Voor de deelnemende AIVD-ers was het een soort cultuurshock om buiten de muren van het AIVD-pand met informatie van de AIVD te werken. Dit maakte dat de samenwerking in een andere vorm werd gegoten: de CT-Infobox. Deze CT-infobox,

door de medewerkers van de AIVD en het KLPD eenvoudigweg 'de box' genoemd, is in het pand van de AIVD gevestigd en valt geheel onder de WIV 2002. De medewerkers van de box zijn dan ook artikel 60 ambtenaren (zie subsectie 3.6.1) Overigens was het volgens diverse respondenten ook een cultuurschok voor de AIVD dat de box binnen de muren van de AIVD werd gehuisvest. Dit betekende immers dat niet-medewerkers van de dienst binnen de muren van de AIVD werkten. Alhoewel zij artikel 60 ambtenaren zijn en formeel vallen onder verantwoordelijkheid en aansturing van de AIVD, werden zij toch gezien als indringers.

"*Je moet wel goed begrijpen: wij waren voor de dienst de indringers. Wij zaten daar als niet-AIVDers in hun pand, iets dat nog nooit eerder was vertoond. In het begin hebben we als box bij de dienst echt moeten vechten om erkenning. Het ging toen zo: 'we weten niet wat we met Mohammed A. aanmoeten, we weten te weinig van hem. Flikker hem maar over de schutting bij de box, dan zien we wel wat er uitkomt'. Dit was natuurlijk nooit de bedoeling van de box. Binnen de box moeten die subjecten worden bekeken die ertoe doen. We hebben die strijd wel gewonnen, nu functioneert de box zoals we in het begin bedoelden."* Interview (voormalig) medewerker AIVD (C), februari 2008.

Inmiddels is de CT-infobox een samenwerkingsverband tussen de AIVD, MIVD, het KLPD, het OM, de Immigratie en Naturalisatiedienst (IND), en de FIOD (de laatste participeert in het kader van een pilot). De NCTb is geen formele partner binnen de box in die zin dat deze geen personeel levert. Zij zijn wel in het algemene bestuur (het zogenoemde 'coördinerend beraad') vertegenwoordigd. Er is geen specifieke wettelijke grondslag voor de CT-infobox: de samenwerking is geregeld bij convenant. Op dit moment wordt er, op advies van de Commissie van Toezicht, aan een wettelijke grondslag in de vorm van een AMvB gewerkt (CTIVD nr 12: 22-24). Zoals gezegd is de WIV 2002 van toepassing op de CT-infobox. Formeel juridisch is de CT-infobox dan ook een onderdeel van de AIVD.

De aansturing van de CT-infobox ligt bij de teamleider CT-infobox. Voorheen is dit vaak een AIVD-er geweest, maar het is de bedoeling om in het kader van de uitgangspunten van gelijkwaardigheid en wederkerigheid ook andere partners die rol te laten vervullen. De uiteindelijke aansturing van de CT-infobox ligt bij het coördinerend beraad, waarin alle deelnemende partijen zijn vertegenwoordigd. Het coördinerend beraad functioneert ook als een soort laatste en hoogste escalatiemogelijkheid: bij problemen kan de teamleider casus voorleggen aan het coördinerend beraad, welke uiteindelijk een definitieve beslissing neemt. Het coördinerend beraad is ook eindverantwoordelijke voor de CT-infobox. In dit opzicht functioneert het dus als een soort bevoegd gezag voor de CT-infobox.

B: De taken van de CT-infobox

De CT-infobox heeft vier taken. Allereerst is zij een schakel tussen de inlichtingendiensten en de opsporing, naast organisaties zoals de RID. Ten tweede genereert de CT-infobox sturingsinformatie voor nieuwe en lopende onderzoeken. Ten derde is zij belast met het coördineren van de activiteiten van de deelnemende organisaties. Ten vierde zorgt de CT-infobox voor gezamenlijke analyses van deelprojecten en signaleert zij trends en ontwikkelingen (Commissie Havermans 2004: 101). De toegevoegde waarde van de CT-infobox ligt met name in het feit dat informatie van de deelnemende partijen met betrekking tot (islamitisch) terrorisme en

daaraan gerelateerde radicalisering op een centraal punt bij elkaar wordt gebracht en vervolgens gecombineerd wordt geanalyseerd. De medewerkers van de CT-infobox hebben voor deze taak de toegang tot de relevante gegevensbestanden van de deelnemende partijen en kunnen deze rechtstreeks en geautomatiseerd raadplegen. De zoekslagen vanuit de CT-infobox worden niet gelogd, omdat ook voor de CT-infobox geldt dat de methoden en informatiepositie afgeschermd dient te blijven. Hierbij is er één kanttekening met betrekking tot de politie-informatie: CIE-informatie is op dit moment nog van de rechtstreekse raadpleging uitgesloten. Dit is dezelfde discussie als de discussie die speelt met betrekking tot artikel 24 WPG.

C: De interne werking van de CT-infobox

De deelnemende partijen zijn alle bevoegd om subjecten aan te dragen van wie zij van mening zijn dat ze in aanmerking komen voor opname in de CT-infobox. De partijen hebben criteria opgesteld volgens welke personen kunnen dan wel moeten worden aangemeld; voor de aanmelding bestaat een specifiek formulier. Omdat de CT-infobox onder de werking van de WIV 2002 valt, gelden voor opname in de CT-infobox in ieder geval dezelfde criteria die gelden voor verwerking door de AIVD. Iemand komt daarom pas in aanmerking voor verwerking indien er een aanleiding is tot een ernstig vermoeden van een gevaar voor de democratische rechtsorde of voor de veiligheid van de staat of andere gewichtige belangen van de staat. In de praktijk melden slechts de AIVD, het KLPD en de MIVD personen aan voor opname in de CT-infobox. Uiteindelijk beslist het teamhoofd van de CT-infobox of iemand wordt opgenomen. Er bestaan overigens ook criteria voor het verwijderen van personen van de lijst van de CT-infobox (zie Van der Bel et al. 2009: 291). Wanneer een subject het land uitgezet is, tot een gevangenisstraf van 12 jaar of meer is veroordeeld, of vanwege andere redenen niet relevant meer is, wordt hij van de lijst gehaald (CTIVD nr. 12: 9-11). Bij de start van de analytische cel stonden er 150 subjecten op de lijst. Hoeveel er nu op staan is niet bekend, maar wellicht zijn dit er inmiddels meer dan 150.

Na de intake wordt er een zogenaamd CV van het subject opgesteld. De deelnemende organisaties brengen informatie omtrent het subject bij elkaar. In het kader van hun AIVD taak krijgen de RID-en een lijst van de in de CT-infobox opgenomen personen. Zij zoeken in de informatie van de regiokorpsen naar relevante informatie. De verstrekking van de lijst aan de RID vindt plaats in het kader van de AIVD-taak van de RID, waarmee het juridisch gezien een interne verstrekking binnen de AIVD is. De CIE-en ontvangen deze lijst niet: het gesloten verstrekkingregime van de WIV 2002 zou daar volgens de commissie van toezicht geen ruimte voor bieden (CTIVD 2007: 9-11). Over de noodzaak en de wenselijkheid hiervan is wel gediscussieerd. Met behulp van de lijst zou de CIE haar eigen informanten gericht kunnen bevragen, hetgeen wellicht belangrijke nieuwe informatie oplevert. Waarom dit niet wenselijk wordt geacht ligt waarschijnlijk in het feit dat de CIE op deze manier te veel inzicht zou kunnen krijgen in de informatiepositie van de AIVD, hetgeen in strijd is met de geheimhoudingsverplichting van die dienst. De AIVD (lees: CT-infobox) mag wel persoonsgegevens aan de CIE verstrekken waarmee de laatste kan nagaan of zij over relevante informatie beschikt. Momenteel wordt er een discussie gevoerd over een directe toegang van medewerkers van de CT-infobox tot zogenoemde 00-gegevens van de CIE.

De gegevens die zijn verzameld omtrent de nieuw aangemelde subjecten worden door de verschillende organisaties die zijn aangesloten bij de box

geanalyseerd, en vervolgens wordt bepaald welke maatregelen gewenst en mogelijk zijn. Hierbij moet men denken aan een inlichtingenmatige, strafrechtelijke, vreemdelingrechtelijke, fiscaalrechtelijke of persoonsgerichte aanpak (bepaalde maatregelen in het kader van de openbare orde onder gezag van de burgemeester). Ook is het mogelijk dat de CT-infobox bepaalde partijen aanraadt om een subject te monitoren omdat de beschikbare informatie te weinig zegt over een wenselijke of noodzakelijke aanpak. De juridische grondslag voor adviezen aan de AIVD en MIVD zijn (1) artikel 35 WIV 2002, die de AIVD-interne gegevensverstrekking regelt, en (2) artikel 58 WIV 2002, die de samenwerking tussen de AIVD en de MIVD regelt (Van der Bel, et al. 2009: 294). De juridische grondslag voor adviezen aan andere partners in de box is artikel 36 WIV 2002. De verstrekking van gegevens aan het OM die van belang kunnen zijn voor de opsporing- en vervolging van strafbare feiten vindt plaats op basis van artikel 38 WIV 2002.

Het is van groot belang om te begrijpen dat de CT-infobox werkt volgens het zogenoemde 'gesloten-box' principe. Aan de CT-infobox verstrekte informatie wordt niet door de CT-infobox aan andere deelnemende partijen doorgegeven (Van der Bel 2009: 291). Indien de CT-infobox meent dat een partij over informatie beschikt die relevant zou kunnen zijn voor een andere partner van de CT-infobox, zal zij een advies doen uitgaan naar de eigenaar van de informatie om tot verstrekking over te gaan. Dit is geen bindend advies en hoeft niet te worden opgevolgd. Er is natuurlijk wel wat uit te leggen als het fout gaat en er een aanslag wordt gepleegd die voorkomen had kunnen worden indien informatie onderling was gedeeld. In de praktijk zullen partijen vrij snel geneigd zijn om het advies op te volgen. Een eventuele verstrekking vindt plaats overeenkomstig de voor de verstrekkende partij relevante wetgeving (voor de politie is dat met name de WPG of de WIV 2002). Volgens enkele respondenten kun je maar beter geen informatie aan de CT-infobox verstrekken omdat je het dan kwijt bent.

"*De tactiek van de dienst bij de infobox was om iedereen artikel 60 ambtenaar te maken. De oorspronkelijke waarde van de dienst is nu weg. Het is een adviesorgaan geworden. Alle informatie in de box is nu AIVD-informatie geworden. Je verstrekt informatie, wilt wat terug, maar dat kan niet omdat iedereen nu artikel 60 is.*" Interview projectmedewerker IGP (A), november 2009.

D: De regionale CT-infoboxen

Het KLPD is één van de partners in de CT-infobox. Terrorismebestrijding is echter iets dat bij veel korpsen plaatsvindt. Zo vonden er in 2010 bij de verschillende korpsen 31 onderzoeken naar terrorisme plaats, waarvan het merendeel bij de regionale politiekorpsen. Rechercheafdelingen, CIE-en, en RID-en kunnen dus allemaal te maken krijgen met terrorisme. Om te zorgen voor afstemming van activiteiten door deze diensten zijn regionale CT-infoboxen opgericht. Alleen in naam vertonen deze boxen gelijkenis met de 'echte' CT-infobox. Feitelijk zijn de regionale CT-infoboxen geen afzonderlijke organisatieonderdelen, maar afstemmings-overleggen tussen verschillende partijen die bij terrorismebestrijding betrokken (kunnen) zijn. Deze regionale CT-infoboxen beschikken dan ook niet over eigen informatiesystemen waarin terrorismerelevante informatie wordt vastgelegd. De bedoeling van de regionale CT-infobox is dat het een afstemmingsoverleg is, niet meer dan dat. Via dit overleg krijgt de RID inzicht in de informatiepositie en de subjecten van de CIE. De CIE krijgt op haar beurt geen zicht in de informatiepositie

en subjecten van de RID. Dit is immers niet mogelijk nu de terrorismebestrijding door de RID valt onder diens AIVD-taak (Van der Bel et al. 2009: 295). Zoals al eerder is beschreven, biedt de WIV 2002 hiertoe niet de mogelijkheid.

E: Is de CT-infobox een echt samenwerkingsverband?

In de CT-infobox is volgens de Commissie een goede modaliteit voor samenwerking gevonden, waarmee anno 2004 een 'werkbare vorm' van operationele samenwerking tot stand zou zijn gekomen (Commissie Havermans 2004: 100-101). De CT-infobox biedt een oplossing voor het echte grote probleem in de vertrouwensrelatie tussen de organisaties: het derde kenmerk van vertrouwen, te weten risico. Toch concludeert de Commissie van Toezicht in 2007 dat het beeld van de CT-infobox als het antwoord op het vertrouwensprobleem niet helemaal klopt. Zo heeft de AIVD zichzelf met name in het begin van de CT-infobox een te grote leidinggevende positie aangemeten, hetgeen de samenwerking op basis van gelijkwaardigheid niet ten goede kwam. Dit beeld kregen wij tijdens ons onderzoek bevestigd.

De bedoeling is dat de CT-infobox ervoor zorgt dat terrorismebestrijding effectiever wordt door onder andere de AIVD en de politie structureel te laten samenwerken. Binnen de CT-infobox zou een situatie van gelijkwaardigheid en wederkerigheid moeten bestaan. De vraag die rijst, is in hoeverre aan deze doelstellingen is voldaan. Volgens diverse respondenten werkt de CT-infobox intern erg goed. De medewerkers van de verschillende organisaties kunnen goed samenwerken en dit komt de gezamenlijke producten ten goede. Er is binnen de CT-infobox sprake van vertrouwen tussen de medewerkers.

"*Binnen de box was er vertrouwen tussen alle medewerkers. Er werd binnen de box dus wel informatie uitgewisseld. Er heerste een enorme saamhorigheid.*" Interview (voormalig) medewerker AIVD, februari 2008.

De vraag die rijst met betrekking tot de CT-infobox is of er wel sprake is van daadwerkelijke samenwerking. Het probleem met de CT-infobox zit namelijk niet zozeer in de interne werking, maar veel meer in de relatie tussen de deelnemende partners in het algemeen. Zo geven oud medewerkers aan dat de AIVD over het algemeen de boventoon voert binnen de CT-infobox. Dit heeft er deels mee te maken dat de leidinggevenden van de AIVD altijd in de CT-infobox of direct in de buurt zijn. De leidinggevenden van de politie zitten op een grotere afstand, hetgeen sommige respondenten doet concluderen dat de politieleiding vaak afwezig is. De AIVD is dan ook vanwege de fysieke locatie van de CT-infobox nauw betrokken bij het reilen en zeilen van de CT-infobox. Een ander probleem is de manier waarop door politiemensen naar de CT-infobox wordt gekeken. Het is volgens de meeste mensen een onderdeel van de AIVD, en de medewerkers van de CT-infobox zijn medewerkers van de AIVD.

"*Kijk, alle mensen in de box zijn feitelijk AIVD-ers. Zo worden ze behandeld, en dat zijn ze eigenlijk ook. Ze krijgen de zwaarste screening, vallen onder aansturing van (de directeur democratische rechtsorde) en zien bijna alles. Iedere medewerker van de box is een artikel 60 ambtenaar, en valt ook onder de WIV. Politiemensen in de box zien dingen die andere politiemensen eigenlijk nooit zullen zien. Toen ik in de box zat, kon ik ook niks tegen collega's vertellen.*" Interview voormalig medewerker AIVD (D), juni 2009.

Een andere medewerker verwoordde het als volgt.

"*(…) De box is een mooi theoretisch verhaal. Ze doen hun best en werken hard, maar het probleem is gewoon waar ze zitten (gebouw van de AIVD; opmerking auteur).*" Interview runner CIE (B), oktober 2008.

Dit beeld wordt overigens ook door de betreffende medewerkers zelf in stand gehouden: ze geven vaak aan dat ze een andere baan hebben en naar de AIVD gaan, ondanks het feit dat ze formeel in dienst van de politie blijven. Vanwege het feit dat de politiemedewerkers van de CT-infobox artikel 60 ambtenaren worden, verliest de politieleiding voor een groot deel sturing en zeggenschap over deze mensen. Ze staan dan nog wel formeel op de formatieplekken van de politie, in de praktijk werken ze voor de AIVD. Dit betekent dan ook dat er van samenwerking en de hiervoor noodzakelijke gelijkwaardigheid geen sprake is. De CT-infobox is voor de politie gewoon AIVD. Dit komt ook omdat de wijze van communicatie door de CT-infobox door middel van ambtsberichten geschiedt. In de wandelgangen verwoordde een politiemedewerker het als volgt: "*als het loopt als een AIVD-er en praat als een AIVD-er, dan is het een AIVD-er*" (sociaal gesprek, juni 2010).

Nu de CT-infobox is verworden tot een onderdeel van de AIVD, is één van de doelstellingen van de CT-infobox niet bereikt: van samenwerking tussen de verschillende organisaties is geen sprake. Wij sluiten ons aan bij de volgende uitspraak uit het rapport Data voor Daadkracht (2006: 67): "*Hoewel de werelden van de inlichtingendiensten en de opsporingsdiensten dus naar elkaar toegroeien, trekken deze diensten zelf vaak nog niet samen op.*" Anno 2012 is dit nog steeds het geval, ondanks het feit dat de CT-infobox intern wel goed functioneert. Vanuit het perspectief van de politie is de CT-infobox hetzelfde als de AIVD, met vergelijkbare problemen. Wij concluderen dan ook dat, alhoewel de CT-infobox zeker succesvol is in de zin dat relevante terrorismegerelateerde informatie wordt samengebracht en gezamenlijk wordt geanalyseerd, er van daadwerkelijke samenwerking geen sprake is. Ook hier komt dat door een gebrek aan onderling vertrouwen: om te kunnen samenwerken in de CT-infobox moesten alle medewerkers de artikel 60 status hebben, en om het helemaal veilig te maken moest de fysieke locatie van de CT-infobox in het pand van de AIVD zijn. Met name de artikel 60 status wordt voorgesteld als een juridische eis (de WIV zou informatie-uitwisseling anders niet mogelijk maken). Alhoewel de juridische basis formeel juridisch de WIV zal moeten zijn (zie CTIVD 2007), neemt het niet weg dat het vasthouden aan de bepalingen van de WIV uiteindelijk voortkomt uit wantrouwen. Wij zijn het dan ook met het CTIVD eens dat er in de nieuwe juridische basis voor de CT-infobox meer uitgegaan moet worden van gelijkwaardigheid (CTIVD 2007: 22-23). Slechts dan kan er sprake zijn van een vertrouwensrelatie tussen de betrokken partijen.

8.12 Hoofdstukconclusie en antwoord op OV4

In dit hoofdstuk geven wij een antwoord op OV 4: *Wat is de verhouding tussen de AIVD en de CIE in de praktijk?* Wij hebben in hoofdstuk twee de conceptuele verschillen tussen de veiligheidsdiensten en de politie behandeld, en in dit hoofdstuk hebben we vastgesteld dat er in theorie met betrekking tot de conceptuele verschillen belangrijke veranderingen zijn opgetreden en binnenkort optreden. Deze veranderingen spelen met name binnen de politieorganisatie. Kort gezegd worden drie van de vier door ons benoemde verschillen steeds kleiner. Ten eerste richt de

politie zich met betrekking tot haar taakstelling in toenemende mate op onderzoeken met een nationaal belang die weinig verschillen van de taak van de veiligheidsdiensten, te weten de bescherming van de nationale veiligheid. Steeds meer gedragingen worden strafbaar gesteld. Met name de ideologische misdrijven waarop de politie zich richt zijn in dit opzicht van belang: voorheen had de politie een marginale rol bij het bestrijden van terrorisme, maar sinds de aanslagen van 11 september 2001 houdt zij zich in toenemende mate bezig met terrorismebestrijding en komt daarmee mogelijk in het vaarwater van de AIVD. Ten tweede verandert het middel waarmee de politie haar taak moet vervullen van waarheidsvinding naar het geven van voorwaarschuwingen. Ten derde treden er veranderingen op in het werkproces: de politie werkt in toenemende mate volgens de intelligencecyclus. Het vierde verschil, de geheimhouding van de AIVD versus de transparantie van de politie, is wat complexer. Enerzijds wordt de transparantie binnen de politie vanwege het *need to share* streven steeds groter, maar aan de andere kant onttrekt de politie zich aan de tirannieke werking van het procesdossier door in toenemende mate gebruik te maken van alternatieven voor een strafrechtelijke aanpak. Vanwege deze theoretische veranderingen zijn er voldoende (theoretische) redenen voor de AIVD en de politie (in ons onderzoek de CIE) om (1) activiteiten onderling op elkaar af te stemmen, (2) informatie te delen en (3) in bepaalde gevallen zelfs samen te werken. Voor deze drie elementen geldt dat in toenemende mate sprake moet zijn van vertrouwen. Wij stellen in dit hoofdstuk vast dat vertrouwen tussen de AIVD en de CIE (en de politie in het algemeen) problematisch is. Twee belangrijke 'ingrediënten' van vertrouwen zijn in de relatie tussen de AIVD en de politie aanwezig: de organisaties staan niet in een materiële hiërarchische verhouding tot elkaar (maar wel in een functionele) en ze hebben genoeg operationele en politieke redenen om een duurzame relatie op te bouwen en in stand te houden. De verregaande geheimhouding aan de kant van de AIVD en de transparantie aan de kant van de politie maken het risico van een mogelijk geschaad vertrouwen echter te groot. De CIE kan er niet op vertrouwen dat de AIVD haar belangen behartigt omdat zij dit, vanwege de geheimhouding, niet kan inschatten. Zoals we in hoofdstuk zeven hebben betoogd, leidt geheimhouding vrijwel automatisch tot negatieve beeldvorming, hetgeen het vertrouwen negatief beïnvloedt. Dit geldt ook voor de verhouding AIVD/CIE. Voor de AIVD geldt nog steeds het risico dat aan de politie verstrekte informatie met teveel mensen wordt gedeeld, zeker indien er volgens het *need to share* denken wordt gehandeld. Dit maakt dat de AIVD de politie niet kan vertrouwen omdat het risico te groot is dat het vertrouwen wordt geschonden. Overigens was het met onze onderzoeksmethode niet mogelijk om vast te stellen van hoeveel vertrouwen er sprake is: dat vereist een kwantitatieve onderzoeksmethode.[295] Maar voor de beantwoording van onze onderzoeksvragen is inzicht in de precieze mate van vertrouwen niet nodig. Wij constateren dat vertrouwen tussen de AIVD en de CIE in algemene zin problematisch is vanwege de mate van geheimhouding over en weer. Dat er sprake is van een bepaalde gradatie van vertrouwen kan volgens ons wel worden afgeleid uit de mate waarin van de hierboven benoemde modaliteiten van interactie sprake is.

Het ontbreken van vertrouwen speelt sterker naarmate de interactie intensiever wordt. Wij stellen daarom vast dat de eerste modaliteit van interactie, de onderlinge afstemming van werkzaamheden, in de praktijk redelijk tot goed verloopt.

[295] Los van het feit dat het ons vrijwel onmogelijk lijkt om een onderzoeksmethode te ontwikkelen waarbij kwantitatief kan worden vastgesteld in welke mate er sprake is van vertrouwen.

Met name in het IOT worden activiteiten afgestemd en de betrokkenen zijn positief over de samenwerking. Het risico is hier dan ook het kleinst, omdat de politie in belangrijke mate invloed en autonomie behoudt. Daarnaast is het overleg zeer kleinschalig, waardoor de aanwezigen sneller een persoonlijke inschatting kunnen maken over met wie ze informatie delen. Er is met andere woorden weinig anonimiteit. Als het echter gaat om de tweede modaliteit van interactie, de informatie-uitwisseling, zien we dat het minder goed verloopt. Vanuit de CIE is er terughoudendheid met betrekking tot het delen van de 00, 200 en 300 informatie met de AIVD omdat dit tot niet in te schatten veiligheidsrisico's leidt. De informatie wordt aan een anonieme partij verstrekt, te weten de AIVD, en wat er verder met de informatie wordt gedaan is niet in te schatten. De laatste modaliteit van samenwerking vergt de meeste openheid en vertrouwen over en weer. Met name de AIVD is terughoudend met daadwerkelijke samenwerking. Wij constateren dat wanneer de eerste poging tot daadwerkelijke effectieve samenwerking, te weten de CT-infobox, wordt bezien vanuit het oogpunt van samenwerking, deze vorm van samenwerking evenwel lijkt te zijn mislukt. De CT-infobox wordt door politiemensen gezien als een onderdeel van de AIVD, en de samenwerking die binnen de CT-infobox plaatsvindt is in hun ogen geen samenwerking tussen de AIVD en de politie. Wij merken hierbij overigens op dat, bezien vanuit het oogpunt van een effectieve terrorismebestrijding, de CT-infobox wel succesvol is. Binnen de CT-infobox komt informatie van de AIVD en de politie in ieder geval samen en het leidt tot adviezen aan de verschillende partijen die zijn betrokken bij terrorismebestrijding. Er zou van een daadwerkelijke samenwerking sprake kunnen zijn indien er meer sprake is van gelijkwaardigheid en de betrokken partijen niet meer vallen onder verantwoordelijkheid en aansturing van de AIVD.

Wij constateren dat de verhouding tussen de AIVD en de CIE (en de politie in het algemeen) nog steeds weinig kenmerken van een vertrouwensrelatie heeft. Pas wanneer er aan alle voorwaarden voor vertrouwen wordt voldaan, kan er daadwerkelijk gewerkt worden aan interactie die verder gaat dan afstemming en marginale informatie-uitwisseling.

9| Conclusies

In dit hoofdstuk geven wij antwoord op de probleemstelling die centraal staat in dit onderzoek. De probleemstelling luidt als volgt.

Wat zijn de gevolgen van de implementatie van het concept van intelligence in de context van de Nederlandse opsporingspraktijk voor de verhouding tussen de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Criminele Inlichtingeneenheid (CIE) van de Nederlandse politie?

Wij beantwoorden de probleemstelling aan de hand van vier centrale onderzoeksvragen. In sectie 9.1 behandelen we de eerste onderzoeksvraag (OV 1). Het antwoord op deze onderzoeksvraag geeft (1) inzicht in de traditionele conceptuele kenmerken en verschillen tussen een veiligheidsdienst en de politie, en (2) geeft aan in hoeverre de AIVD en de CIE aan deze kenmerken voldoen. Vervolgens behandelen we in sectie 9.2 de tweede onderzoeksvraag (OV 2). Het antwoord op deze vraag geeft inzicht in het concept IGP en de manier waarop dit concept de traditionele politie in theorie zou moeten veranderen. Wij willen echter niet alleen inzicht hebben in het concept IGP, maar ook in hoe dat concept in de CIE-praktijk wordt geïmplementeerd. Dat behandelen we in sectie 9.3, waarin we de derde onderzoeksvraag (OV 3) beantwoorden. Sectie 9.4 geeft een antwoord op de vierde onderzoeksvraag (OV4). Het antwoord op deze laatste onderzoeksvraag geeft inzicht in de verhouding tussen de AIVD en de CIE in de praktijk. Het gaat verder waar de eerste onderzoeksvraag stopte. OV 4 behandelt niet zozeer de verschillen tussen de AIVD en de CIE, maar geeft inzicht in de wijze waarop deze organisaties invulling geven aan de onderlinge interactie in de praktijk van terrorismebestrijding.

In sectie 9.5 bezien we in hoeverre de antwoorden op de vier onderzoeksvragen leiden tot een (begin van een) antwoord op de centrale probleemstelling. In sectie 9.6 geven we een aanzet tot een discussie omtrent de onderwerpen waar wij onderzoek naar hebben gedaan. We sluiten in sectie 9.7 het hoofdstuk en daarmee deze studie af met een slotbeschouwing.

9.1 De conceptuele verhouding tussen de AIVD en de CIE

Onze eerste onderzoeksvraag (OV1) luidt als volgt.

Wat zijn de traditionele kenmerken van een veiligheidsdienst en de politie?

We hebben in het inleidende hoofdstuk vastgesteld dat in het Angelsaksisch systeem, waarop het Nederlandse systeem is gebaseerd, de veiligheidsdiensten en de politie van elkaar gescheiden zijn. Deze scheiding heeft tot belangrijke verschillen tussen de organisaties geleid. Voor beide organisaties hebben wij vier soorten kenmerken benoemd, te weten (A) de algemene taakstelling, (B) het middel waarmee ze de taak uitvoeren, (C) het werkproces, en (D) de relatie met externen. Aan de hand van deze kenmerken wordt duidelijk in welke opzichten de organisaties van elkaar verschillen.

A: De algemene taakstelling

We hebben vastgesteld dat de algemene taak van een veiligheidsdienst de bescherming van de nationale veiligheid is (HP-kenmerk 1). Een veiligheidsdienst heeft een behoorlijke vrijheid bij het beoordelen welke gevallen onder deze taakstelling vallen. De politie richt zich op het handhaven van de strafrechtrechtelijke rechtsorde, oftewel de criminaliteitsbestrijding (LP-kenmerk 1). Deze strafrechtelijke rechtsorde wordt gevormd door vooraf door de wetgever vastgestelde strafrechtelijke bepalingen. Daar waar de veiligheidsdienst dus veel ruimte heeft voor het invullen van zijn taak, kan de politie slechts optreden tegen de gedragingen die vallen onder de door de wetgever vooraf vastgestelde criteria welke zijn vervat in delictsomschrijvingen. Met andere woorden: wat tot de rechtsorde behoort, volgt uit door de wetgever vastgestelde normen. De politie heeft hierbij geen rol. Wat tot de nationale veiligheid moet worden gerekend, wordt in de praktijk echter door de veiligheidsdiensten zelf ingevuld: er is geen wetboek waarin de normen ten behoeve van de nationale veiligheid zijn opgenomen. In hoeverre gelden deze kenmerken voor respectievelijk de AIVD en de CIE?

We constateren dat het bovengenoemde eerste kenmerk van een inlichtingen- en veiligheidsdienst ook voor de AIVD geldt. Dit volgt uit artikel 6 lid 1 sub a WIV 2002, waarin de AIVD in het kader van de bescherming van de nationale veiligheid de taak krijgt om onderzoek te verrichten naar bedreigingen van de democratische rechtsorde of de veiligheid en andere gewichtige belangen van de staat. 'Nationale veiligheid' is een open begrip en wordt door de AIVD zelfstandig ingevuld.

Voorts stellen wij vast dat de algemene taakstelling van de politie, te weten de handhaving van de strafrechtelijke rechtsorde, ook voor de CIE geldt. De CIE is een onderdeel van de politieorganisatie en ontleent haar taak aan de wettelijke taakstelling van de politie in het algemeen en de CIE-regeling in het bijzonder. De algemene taakstellende wettelijke bepaling voor de politie in het algemeen is artikel 2 Politiewet 1993, waarin onder meer wordt gesteld dat de politie is belast met de strafrechtelijke handhaving van de rechtsorde. Uit artikel 2 van de CIE-regeling volgt voorts dat de CIE belast is met de informatievoorziening in het kader van de uitvoering van de politietaak met betrekking tot de zware en georganiseerde criminaliteit en terrorisme. Alhoewel de CIE haar werkzaamheden in een vroege fase van het strafproces verricht, vallen deze nog steeds onder de strafrechtelijke handhaving van de rechtsorde. Omdat de rechtsorde mede wordt gevormd door van tevoren door de wetgever geformuleerde delictsomschrijvingen, is het de CIE niet toegestaan om zich bezig te houden met gedragingen die niet strafbaar zijn gesteld.

B: Het middel

Met betrekking tot het tweede algemene kenmerk van de veiligheidsdiensten hebben we gezien dat deze de nationale veiligheid beschermen door middel van het geven van voorwaarschuwingen (HP-kenmerk 2). Omdat een aantasting van de nationale veiligheid grote gevolgen heeft, zal een veiligheidsdienst hierop anticiperen en zoveel mogelijk proberen deze aantasting te voorkomen. Dit maakt dat een veiligheidsdienst proactief en preventief handelt, en de opbouw en instandhouding van een informatiepositie als zelfstandig doel heeft. Omdat de bedreigingen van de nationale veiligheid niet van tevoren zijn bepaald en dus ongekend zijn, is de informatiepositie van de inlichtingen- en veiligheidsdienst feitelijk onbegrensd. Zij

richten zich met andere woorden op een ongekende dreiging. Wij constateerden hier een groot verschil met de politie.

De politie handhaaft de strafrechtelijke rechtsorde door middel van waarheidsvinding en treedt ook daadwerkelijk op tegen geconstateerde schendingen. De strafprocesrechtelijke waarheidsvinding hebben wij gedefinieerd als het onderzoek verricht door de politie naar wat er feitelijk is gebeurd met betrekking tot één of meer strafbare feiten. De politie probeert de materiële waarheid vast te stellen aan de hand van het verzamelen van bewijs. Zij construeert hiertoe allereerst een verhaal omtrent hetgeen is gebeurd, en aan de hand van concreet bewijs wordt dit verhaal al dan niet bevestigd. De strafprocesrechtelijke waarheidsvinding betreft per definitie het verleden, en de politie is dan ook een reactieve organisatie: zij reageert met name op concrete schendingen van de rechtsorde. Het opbouwen en in stand houden van een informatiepositie door de politie zijn begrensd: de verzamelde informatie moet gerelateerd zijn aan de handhaving van de rechtsorde. Het moet gaan om informatie die is gerelateerd aan concrete, strafbare gedragingen. De politie richt zich in dit opzicht op een geconstateerde of gekende dreiging. De vraag is nu in hoeverre de hiervoor genoemde theoretische HP- en LP-kenmerken opgaan voor de Nederlandse veiligheidsdienst AIVD en de CIE van de politie. We beginnen met de AIVD.

Met betrekking tot de AIVD stelden wij vast dat deze dienst zich richt op het geven van voorwaarschuwingen en het proactief signaleren van bedreigingen van de nationale veiligheid. De verschillende bevoegdheden van de AIVD zijn allemaal gericht op informatieverzameling: het opbouwen en in stand houden van een informatiepositie is de belangrijkste activiteit van de AIVD. Dit volgt ook uit artikel 6 WIV 2002, waarin wordt gesteld dat de AIVD 'onderzoek doet' en dus niet dat zij zelfstandig ingrijpt.

Wij constateerden met betrekking tot de CIE dat zij een tweeledige taak heeft. Zij is belast met (1) het verzamelen van informatie door middel van het runnen van informanten en (2) het verkrijgen van inzicht in zware, georganiseerde criminaliteit en terrorisme. In de praktijk richt de CIE zich grotendeels op het runnen van informanten en de verzamelde informatie wordt met name verstrekt aan de tactische opsporingsteams. De CIE is in dit opzicht ondersteunend aan de tactische opsporingsonderzoeken. De tweede taak (ook wel analysetaak genoemd) komt dicht in de buurt bij de AIVD-taak in die zin dat de CIE inzicht in de ontwikkelingen in zware, georganiseerde criminaliteit en terrorisme dient te krijgen. Dit is een taak die een proactieve houding van de CIE vergt. In de praktijk wordt deze taak echter nauwelijks uitgevoerd. Wij stelden dan ook vast dat het tweede traditionele kenmerk van de politie ook voor de CIE geldt: de CIE is met name gericht op waarheidsvinding.

C: Het werkproces

Het derde kenmerk ziet op het werkproces van de organisaties. Om te kunnen komen tot voorwaarschuwingen, moet de verzamelde informatie worden geduid. Dit vereist een verregaand gestructureerd werkproces en een mate van interpretatie van informatie die overeenkomsten vertoont met wetenschappelijke methoden van werken: de intelligence-cyclus (HP-kenmerk 3). Wij hebben de bestaande, traditionele intelligence-cyclus aangepast en komen tot de volgende stappen: (1) de beleidsomgeving heeft bepaalde inlichtingenbehoeften die worden meegenomen bij (2) het opstellen van een intelligence-agenda voor de veiligheidsdiensten. De veiligheidsdiensten gaan over tot (3) het verzamelen, (4) het verwerken en (5) de

analyse van inlichtingen, teneinde tot intelligenceproducten te komen. Daarna (6) worden de analyseproducten verspreid, hetgeen leidt tot (7) het opstellen, bijstellen en implementeren van beleid. Dit beleid heeft invloed op (8) de algemene context van de beleidsomgeving en de veiligheidsdiensten, hetgeen weer leidt tot nieuwe inlichtingenbehoeften bij de beleidsomgeving.

Wij hebben geconstateerd dat de politie volgens het proces van het opsporingsonderzoek (LP-kenmerk 3) werkt. De politie verzamelt bewijs ten behoeve van verdenkingen en veronderstellingen omtrent gepleegde strafbare feiten, teneinde een verdachte aan te houden en deze te (laten) vervolgen. Een belangrijk kenmerk van het opsporingsproces is dat dit gehele proces in verregaande mate is gereguleerd. Niet alleen de waarheidsvinding zelf is ingekaderd door het strafprocesrecht (het gaat immers om het vaststellen van de juridisch relevante waarheid), ook de wijze waarop de politie de waarheid tracht te achterhalen is gebonden aan wettelijke normen en voorschriften.

Het verzamelen van informatie en bewijs ten behoeve van waarheidsvinding verschilt veel van het verzamelen, verwerken en analyseren van informatie ten behoeve van risico-inschattingen (intelligence). Dit maakt het traditionele opsporingsproces doorgaans veel minder gestuurd en gestructureerd. De rechercheur is dan ook traditioneel degene die is belast met het verzamelen, verwerken en analyseren van informatie en er is weinig specialistische expertise. Ook hier rijst de vraag in hoeverre het bovenstaande geldt voor respectievelijk de AIVD en CIE.

Wij stelden vast dat het bijzonder moeilijk is om inzicht te krijgen in de manier van werken door de AIVD. Wij konden dan ook niet zelf vaststellen in hoeverre de AIVD volgens de intelligence-cyclus werkt. Onze respondenten geven wel aan dat de AIVD volgens een dergelijk gestructureerd proces werkt, en geven ook aan dat er bij de AIVD veel aandacht is voor het gebruik van specialistische expertise. Wij gaan er dan ook van uit dat de AIVD volgens de intelligence-cyclus werkt.

Wij constateerden voorts ook dat het CIE-proces in het algemeen deel uitmaakt van het bredere opsporingsproces. De CIE ondersteunt de tactische opsporing bij de waarheidsvinding door inlichtingen te verzamelen die gebruikt kunnen worden als start- en sturingsinformatie. Evenals de tactische opsporing, (1) is het CIE-proces weinig gestructureerd, (2) zijn runners belast met het verzamelen, verwerken en interpreteren van de verzamelde inlichtingen, en (3) worden ook de activiteiten van de CIE in verregaande mate gereguleerd. LP-kenmerk 3 gaat dus in belangrijke mate ook op voor de CIE.

D: De relatie met externen

Voor de veiligheidsdienst wordt de relatie met externen gekenmerkt door een verregaande mate van geheimhouding. Dit is HP-kenmerk vier van de veiligheidsdienst. Geheimhouding heeft *grosso modo* drie redenen: (1) institutionele redenen, (2) sociale redenen en (3) operationele redenen. Wij hebben ons met name op de institutionele redenen en de operationele redenen gericht.

Institutionele redenen voor geheimhouding geven een verklaring voor geheimhouding tussen bureaucratische organisaties. Deze redenen zijn doorgaans (1) het behouden van invloed, (2) het beschermen van autonomie en (3) het risico-averse gedrag van de bureaucratische organisatie in het algemeen. De operationele redenen voor geheimhouding hebben te maken met het afschermen van de informatiepositie en het beschermen van de veiligheid van informatiebronnen zoals informanten en agenten. Formeel worden vaak operationele redenen aangehaald als verklaring voor

verregaande geheimhouding (zowel door de veiligheidsdiensten als door de politie), maar in de praktijk lopen de drie redenen door elkaar heen.

Wij hebben vastgesteld dat het vierde kenmerk van de politie transparantie is. Het optreden van de politie maakt vaak een inbreuk op de rechten van een individu, bijvoorbeeld op het vrijheidsrecht in geval van een aanhouding of het privacyrecht in geval van surveillance-activiteiten (zoals een telefoontap). Uiteindelijk dienen dergelijke inbreuken transparant te zijn: uiteindelijk moet het politie-optreden kunnen worden getoetst door bijvoorbeeld een strafrechter. Dit laat overigens onverlet dat ook de politie bij het uitvoeren van opsporingsonderzoeken of CIE-onderzoeken geheimhouding kan en mag betrachten, maar deze geheimhouding is niet absoluut. De strafrechter dient te weten welke feiten de politie heeft verzameld en hoe zij dat heeft gedaan, en de verdachte moet zich kunnen verweren tegen hetgeen hem ten laste wordt gelegd. Daarnaast is er ook dikwijls transparantie naar de buitenwereld toe. Dit zijn de zogenoemde principes van interne en externe openbaarheid. In de wereld van de veiligheidsdiensten wordt dit ook wel 'de tirannieke werking van het procesdossier' genoemd, en daar bestaat de (terechte) angst dat indien informatie met de politie wordt gedeeld, dit uiteindelijk in een strafdossier terecht komt en daarmee op straat. Dit heeft invloed op de verhouding tussen de veiligheidsdiensten en de politie, zoals we kunnen zien wanneer we de AIVD en de CIE nader bekijken.

Met betrekking tot de AIVD constateerden wij dat deze dienst gebonden is aan een verregaande geheimhouding die is gecodificeerd in artikel 15 WIV 2002. In bepaalde gevallen verstrekt de AIVD informatie aan andere organisaties: de AIVD moet immers voorwaarschuwingen aan anderen geven en die andere partijen moeten vervolgens daadwerkelijk optreden. Er is echter sprake van een gesloten verstrekkingsregime: informatie kan slechts worden verstrekt indien hiervoor een expliciete wettelijke basis bestaat, en deze wettelijke basis is vrij beperkt. Slechts in bepaalde gevallen is het de AIVD toegestaan om af te wijken van deze geheimhouding: verstrekkingen ten behoeve van de opsporing worden in artikel 38 WIV 2002 mogelijk gemaakt. Dit gebeurt in de vorm van een ambtsbericht. Daarin staat zeer summier aangegeven wat de waarschuwing inhoudt. Ook in de ambtsberichten betracht de AIVD dus een verregaande mate van geheimhouding.

Met betrekking tot het laatste kenmerk stelden wij vast dat de CIE deels afwijkt van de politie in het algemeen. Een CIE kent namelijk ook een grote mate van geheimhouding omdat zij de identiteit van informanten dient af te schermen. Door middel van een systeem van coderingen schermt de CIE de meest gevoelige informatie af (dat is met name informatie die kan leiden tot de identificatie van een informant). De geheimhouding door de CIE is echter niet absoluut: de rechter kan van de hoofdregel van geheimhouding afwijken en transparantie van de CIE eisen. Indien informatie wordt gebruikt in een strafproces (als start- of sturingsinformatie), dan kan een strafrechter bijvoorbeeld besluiten dat hij de runners wil horen of zelfs dat hij de identiteit van een informant wil weten. Dit zorgt ervoor dat ook de CIE, zij het in verminderde mate in vergelijking met de rest van de politie, in de ogen van veiligheidsdiensten onderhevig is aan de hiervoor benoemde 'tirannieke werking van het procesdossier'. Ten opzichte van externen betracht de CIE echter een verregaande mate van geheimhouding. Voor ons onderzoek betekent dit dat (1) de CIE in de ogen van de AIVD gewoon een onderdeel is van de politie, met alle risico's van dien als het gaat om transparantie, maar (2) ook dat de CIE ten opzichte van externe partijen, waaronder eveneens de AIVD, een verregaande mate van geheimhouding betracht. Dit heeft gevolgen voor de relatie met deze externe partijen. In dit opzicht vertoont de CIE dus veel overeenkomsten met de veiligheidsdiensten. De eerste bevinding speelt

een rol bij de verhouding tussen de AIVD en de CIE, en de tweede bij de implementatie van IGP.

9.2 Het concept IGP

In deze sectie behandelen wij OV 2. Deze luidt als volgt.

Wat is het concept IGP en hoe beoogt dit concept de traditionele Nederlandse CIE te veranderen?

De politie ziet zich vandaag de dag geconfronteerd met een enorme schaalvergroting. Ten eerste beslaat het strafrecht veel meer activiteiten dan vroeger waardoor de politie zich op veel verschillende onderwerpen moet richten. Ten tweede krijgt de politie steeds meer bevoegdheden waardoor zij in een eerder stadium informatie kan verzamelen, hetgeen leidt tot een toename van de hoeveelheid informatie die verzameld dient te worden. Ten derde betekenen de toenemende digitalisering en de groei van ICT dat er voortdurend meer informatie te verzamelen is en verzameld kan worden. Deze drie redenen leiden gezamenlijk tot een schaalvergroting waaraan de politie zich dient aan te passen. Naast deze schaalvergroting heeft de samenleving in het algemeen en het strafrecht in het bijzonder belangrijke veranderingen ondergaan. Er is in toenemende mate sprake van een risicosamenleving waarin van de politie wordt verwacht dat zij criminaliteit voorkomt in plaats van dat zij criminaliteit opspoort. Daarnaast vereisen de georganiseerde criminaliteit en het terrorisme een proactievere benadering van de politie. De schaalvergroting gecombineerd met de eis van proactiviteit vraagt van de politie een herziening van de manier waarop zij reeds een lange tijd functioneert. Met andere woorden: er is een paradigmawijziging nodig. Van een reactieve, incidentgestuurde organisatie moet de politie intelligence-gestuurd en proactief gaan werken. Door middel van de implementatie van intelligence denkt de politieorganisatie dat te gaan bereiken.

Er zijn veel benaderingen en definities van intelligence. Wij hanteren de conceptbenadering van Gill en Phythian, en definiëren intelligence als volgt: "(intelligence is) *de overkoepelende term voor de reeks van activiteiten – van het vaststellen van een inlichtingenbehoefte en het verzamelen van informatie tot analyse en verspreiding – die in het geheim plaatsvinden en die erop zijn gericht op het bewaken of vergroten van de veiligheid door middel van het geven van voorwaarschuwingen voor bedreigingen of potentiële bedreigingen op een manier die ruimte biedt voor een tijdige implementatie van een preventief beleid of strategie (…).*" IGP is volgens ons de implementatie van dit concept van intelligence in de context van de politie.

De politie focust met name op de implementatie van het werkproces van intelligence, te weten de intelligence-cyclus. Door middel van dat proces hoopt zij te komen tot een proactieve benadering en voorwaarschuwingen. De intelligence-cyclus hebben wij eerder omschreven als een gestructureerd, vraaggestuurd proces waarbij met name de analysefase een belangrijke rol speelt. IGP gaat dan ook uit van (1) de sturing van het politiewerk, hetgeen (2) plaatsvindt op basis van criminaliteitsanalyse. Criminaliteitsanalyse vormt het hart (of beter: het brein) van IGP, leidt tot de opbouw en instandhouding van een politiële informatiepositie en maakt het mogelijk om voorwaarschuwingen te genereren. De sturing houdt kort gezegd in dat er met en op informatie wordt gestuurd. Voorts gaat het concept ook uit van (3) het zoveel mogelijk delen van informatie. Dit alles uiteindelijk ten behoeve van (4) een

proactieve en preventieve aanpak van criminaliteit en terrorisme. De schaal waarmee IGP geïmplementeerd wordt, maakt haar uniek. Het is niet zozeer het idee dat besluitvorming zoveel mogelijk gebaseerd moet zijn op objectieve feiten wat IGP nieuw maakt, maar de omvang waarmee een standaardisering en uniformering van het politiewerk worden beoogd. IGP is een herziening van het gehele politiebestel: het verandert de wijze waarop de politie te werk gaat.

Vergeleken met de hierboven genoemde vier traditionele LP-kenmerken van de politie en de CIE, is IGP dan ook een hele grote verandering. Van de vier traditionele LP-kenmerken moeten er drie veranderen (kenmerken 2, 3 en 4). Het eerste kenmerk, de taakstelling, blijft binnen IGP ongewijzigd: ook de intelligencegestuurde politie richt zich op de strafrechtelijke handhaving van de rechtsorde. Het middel waarmee ze dat probeert te bereiken, verandert wel aanzienlijk van waarheidsvinding naar voorwaarschuwingen.[296] In het werkproces treedt vervolgens de belangrijkste verandering op: er zal volgens de intelligencecyclus gewerkt moeten gaan worden. De CIE zal dus gestructureerd en vraaggestuurd moeten gaan werken, en daarnaast zorgen dat er analysecapaciteit binnen de CIE komt. Als laatste zal de CIE meer informatie moeten gaan delen.

Het tweede onderdeel van OV 2 is de vraag hoe IGP de CIE dient te veranderen. In Nederland is gekozen voor een *top down* benadering waarbij in opdracht van de Raad van Hoofdcommissarissen (RvHC) een procesmodel is opgesteld dat vervolgens dwingend is opgelegd aan de korpsen. Het procesmodel geldt ook voor de CIE. De uitwerking van het procesmodel is genaamd NIM, en de CIE zal zich aan het NIM moeten conformeren om volgens IGP te werken. De genoemde vier kenmerken van IGP komen duidelijk terug in het NIM, maar het NIM voegt hier ook nog bepaalde kenmerken aan toe die fungeren als randvoorwaarden voor een succesvolle implementatie van IGP. Zo wordt (1) de sturing op strategisch niveau vormgegeven door een uitgebreid stelsel van stuurgroepen en op tactisch en operationeel niveau door middel van een systeem van briefen en debriefen, en (2) krijgt de ontwikkeling van criminaliteitsanalyse in RIO's een belangrijke rol. Voorts wordt (3) de nadruk gelegd op het veranderen van de politiecultuur van *need to know* naar *need to share*. Bij het tweede en derde kenmerk voegt het NIM een belangrijke randvoorwaarde toe: (4) de ontwikkeling van een adequate ICT-infrastructuur. In het visiedocument van het NIM wordt vervolgens aangegeven dat de besluitvorming binnen IGP (5) proactief in plaats van reactief is. Door middel van het implementeren van het NIM moet de politie intelligence-gestuurd werken. In de volgende sectie behandelen wij in hoeverre dit in de CIE-praktijk is gelukt.

9.3 IGP in de praktijk

In deze sectie behandelen wij OV3. Deze onderzoeksvraag ziet op de praktijk van IGP en luidt als volgt.

In hoeverre is IGP geïmplementeerd in de Nederlandse CIE-praktijk?

Wij hebben onderzocht in hoeverre de bovengenoemde *top down* benadering van het NIM effect heeft gesorteerd bij de CIE, en kwamen tot de conclusie dat er drie

[296] Overigens willen wij hiermee niet suggereren dat er helemaal geen ruimte meer is voor de traditionele waarheidsvinding. IGP zal de voorwaarschuwing weliswaar van een veel groter belang maken dan thans het geval is, maar de opsporing van strafbare feiten blijft een essentieel onderdeel van het politiewerk.

algemene redenen zijn die een succesvolle implementatie van IGP in de weg staan. Wij behandelen in subsectie 9.3.1 deze drie algemene barrières tegen een succesvolle implementatie van IGP die wij hebben geïdentificeerd. Daarna zullen wij in subsectie 9.3.2 aangeven in hoeverre deze redenen een rol spelen bij de implementatie van de hierboven genoemde elementen van het NIM binnen de CIE. In 9.3.3 sluiten wij de sectie af met een conclusie.

9.3.1 Algemene barrières voor een succesvolle implementatie van IGP

De algemene barrières tegen een succesvolle implementatie van IGP zijn achtereenvolgens (A) de onduidelijkheid omtrent IGP en wat het concept beoogt te bereiken, (B) hardnekkige structuurkenmerken van de politie en (C) de weerbarstige politiecultuur.

A: Onduidelijkheid omtrent IGP

Wij constateerden dat het concept IGP op de werkvloer wel bekend is, maar dat er verschillen bestaan in wat mensen eronder verstaan. Het is volgens sommigen een modeterm, en volgens anderen een compleet andere manier van werken. De door ons geconstateerde onduidelijkheid omtrent IGP volgt allereerst uit de praktijk binnen de politie door het label 'intelligence-gestuurd' voor veel verschillende onderwerpen te gebruiken; men spreekt van IGO, IGP en IGV. Dit leidt tot een *netwidening* die de implementatie van het concept bemoeilijkt. De vraag rijst immers wat er precies moet worden geïmplementeerd.

Een tweede verklaring voor de onduidelijkheid ligt in het verlengde van de *netwidening*. Er is inmiddels zoveel informatie binnen de politie beschikbaar over elementen van IGP dat de medewerkers niet meer kunnen inschatten wat wel en wat niet bij IGP hoort. Ze zien door de bomen het bos niet meer. Leidinggevenden gebruiken termen als 'aan de voorkant zitten', maar deze termen zijn voor een medewerker op de werkvloer weinig verhelderend.

De onduidelijkheid omtrent IGP komt daarnaast ook voor een deel voort uit onbekendheid met de complexiteit van interne processen en de interne dynamiek binnen de politieorganisatie in het algemeen. Zaken worden geproblematiseerd zonder dat er een daadwerkelijke probleemanalyse aan ten grondslag ligt. Dit leidt ertoe dat oplossingen worden aangedragen die niet goed aansluiten op de daadwerkelijke problemen binnen de politieorganisatie. IGP is een favoriete oplossing geworden voor veel problemen, een soort wonderzalf voor allerlei kwalen. Dit heeft in voorkomende gevallen echter niet zelden een onbedoeld neveneffect en kan bepaalde problemen juist verergeren in plaats van oplossen.

B: Hardnekkige structuurkenmerken

Een structuurkenmerk komt voort uit de inrichting en vormgeving van de politieorganisatie. Structuurkenmerken zijn met de organisatie verbonden en laten zich dan ook niet gemakkelijk veranderen. Het veranderen van structuurkenmerken vergt bijzonder grote inspanningen en een lange-termijn-planning. Voor een 'paradigmawijziging' als IGP is dit echter noodzakelijk. Wij signaleerden de volgende drie essentiële structuurkenmerken die voor IGP problematisch zijn: (1) een grote fragmentatie binnen de politieorganisatie, waardoor autonome machtsblokken

zijn ontstaan, (2) onderlinge concurrentie tussen de verschillende afdelingen binnen de politie en (3) een feitelijke hiërarchie die van de formele hiërarchie afwijkt.

Met betrekking tot het eerste structuurkenmerk constateren wij dat 'de politieorganisatie' feitelijk niet bestaat. De politie valt uiteen in veel verschillende suborganisaties die allemaal een zekere mate van autonomie hebben. Dit geldt voor alle niveaus van de politieorganisatie. Het bestaan van 25 regiokorpsen en een KLPD heeft geleid tot 26 'koninkrijkjes', met bijvoorbeeld elk een eigen leidinggevend kader, eigen ICT-systemen en eigen prioriteiten.[297] Niet zelden is er tussen de korpsen onderling sprake van een bepaalde mate van concurrentie. Maar ook binnen de korpsen vindt een dergelijke fragmentatie plaats. Zo is er binnen de recherche van een typisch regiokorps sprake van veel verschillende organisatieonderdelen die niet zelden een zekere mate van autonomie hebben. De CIE is hier een voorbeeld van. Het probleem met autonome machtsblokken is dat zij bepaalde elementen van een veranderingsproces kunnen tegenwerken wanneer ze van mening zijn dat deze elementen voor hen nadelig kunnen zijn (of voordelig voor de andere organisatieonderdelen). Daarnaast worden concepten als IGP per afdeling opnieuw geïnterpreteerd, en iedere afdeling legt weer andere accenten of verandert het concept dusdanig dat het in lijn ligt met de wens van de betreffende afdeling. Gefragmenteerde autonome eenheden leiden op deze manier tot gefragmenteerd beleid, en een gefragmenteerd beleid is, vanuit het perspectief van het oorspronkelijke beleid, inefficiënt en ineffectief. Voor IGP kan dit betekenen dat de elementen door de verschillende organisatieonderdelen verschillend wordt geïnterpreteerd en geïmplementeerd. De vraag is in hoeverre er dan nog sprake is van IGP zoals het oorspronkelijk is bedoeld. Overigens draagt deze situatie bij tot de hierboven beschreven onduidelijkheid omtrent IGP en het proces van *netwidening.*

Met betrekking tot het tweede structuurprobleem stelden wij vast dat dit vaak het gevolg is van de situatie dat verschillende bureaucratische organisaties vergelijkbare taken hebben. Ze moeten echter strijden om budgetten, invloed en autonomie. Een belangrijk machtsmiddel in de concurrentiestrijd is informatie, hetgeen leidt tot een verregaande afscherming ten opzichte van de concurrentie. De politie is een bureaucratische organisatie met veel interne afdelingen en subculturen die vergelijkbare taken vervullen. Zo is de CIE belast met de informatievoorziening met betrekking tot zware, georganiseerde criminaliteit en terrorisme. Er worden echter ook RIO's in het leven geroepen die een vergelijkbare taak krijgen en daarnaast beschikken over meer analysecapaciteit. Deze zijn echter weer afhankelijk van de CIE en de tactische onderzoeksteams voor de relevante informatievoorziening. Dit is een recept voor onderlinge concurrentie en machtsstrijd waarbij de inzet met name informatie is.

Met betrekking tot het derde structuurprobleem constateerden wij dat de politie een *street-level bureaucracy* is. In de praktijk wordt de politieorganisatie gekenmerkt door een grote discretionaire ruimte voor de medewerkers die formeel het laagste in de hiërarchie staan. Dit volgt uit de aard van het politiewerk: de meeste werkzaamheden van de lagere politiemedewerkers vinden buiten het bereik van de leidinggevenden plaats, waardoor effectieve sturing eigenlijk niet mogelijk is. Met IGP wordt geprobeerd om deze feitelijke hiërarchie te doorbreken en *top-down* veranderingen door te voeren. Dergelijke sturing vanuit de hiërarchie is bij een *street-level bureaucracy* zoals de politie erg moeilijk: de aantasting van de vrijheid van de

[297] Het is ons bekend dat de minister van veiligheid en justitie heeft voorgesteld om een nationale politie op te richten. Wij zien het niet als onze taak om daarop in deze analyse vooruit te lopen, behoudens een korte behandeling in de discussie (subsectie 9.6.1).

medewerker kan leiden tot verzetshandelingen die nauwelijks te bestrijden zijn. De discretionaire ruimte is namelijk inherent aan het 'klassieke' politiewerk, en kan niet van bovenaf doorbroken worden. Dit vereist een andere, slimmere benadering waarbij de werkvloer wordt meegenomen in de veranderingen zonder dat de autonomie van de individuele medewerker wordt aangetast.

C: De weerbarstige politiecultuur

Net als structuurkenmerken zijn cultuurkenmerken bijzonder lastig om op te lossen. Dit komt omdat een cultuur ongrijpbaar is. Cultuur is volgens ons "*de collectieve constructie van de sociale realiteit"*. Dit bestaat uit de manier waarop politiemensen naar de wereld kijken en hoe ze zich vervolgens in de wereld manifesteren. De CIE heeft een aantal cultuurkenmerken die een succesvolle implementatie van IGP in de weg staan.

Allereerst zijn CIE-ers doorgaans conservatief en niet snel geneigd om mee te gaan in veranderingen. Innovaties en ontwikkelingen gaan binnen de CIE daarom erg langzaam. Voor een paradigmawijziging zoals IGP is dit een behoorlijke barrière: het belemmert de acceptatie van nieuwe ideeën en werkwijzen. Een natuurlijk verloop binnen de CIE zal dit overigens veranderen.

Een tweede, hardnekkig cultuurelement ziet op een ander aspect van de mentaliteit van de gemiddelde CIE-medewerker. Veel politiemedewerkers zijn gevormd door het traditionele, reactieve politiewerk en laten zich hierdoor (bewust of onbewust) leiden bij het nemen van beslissingen. Met andere woorden: zij worden geregeerd door een waan-van-de-dag-mentaliteit. Deze mentaliteit zorgt er bijvoorbeeld voor dat strategische lange-termijn-beslissingen zelden worden genomen en dat er van proactiviteit nauwelijks sprake is. Dit zijn beide essentiële kenmerken van IGP. Overigens is een zekere mate van waan van de dag niet uit te sluiten: de politieorganisatie zal altijd worden geconfronteerd met omstandigheden en gebeurtenissen die zij niet heeft (kunnen) voorzien.

Het derde kenmerk is wat binnen de politieorganisatie bekend staat als de *need to know*-cultuur: een cultuur van ongerechtvaardigde geheimhouding. Deze collectieve constructie van de sociale realiteit met betrekking tot anderen die geheimhouding betrachten gaat namelijk uit van het beeld dat er tot op zekere hoogte sprake is van ongerechtvaardigde geheimhouding. Dat wil niet zeggen dat de geheimhouding in werkelijkheid ongerechtvaardigd is: het enkele bestaan van geheimhouding doet anderen reeds vermoeden dat deze geheimhouding in ieder geval deels ongerechtvaardigd is. Zelfs al worden alle ongerechtvaardigde redenen voor geheimhouding weggenomen en zijn er alleen nog maar gerechtvaardigde redenen, dan nog is geheimhouding in de perceptie van degenen voor wie iets geheim wordt gehouden al snel ongerechtvaardigd. Dit laat duidelijk zien wat het probleem van de cultuur is: het gaat om een perceptie van de werkelijkheid met een paradoxale werking, en dergelijke percepties zijn erg moeilijk te beïnvloeden. De politiecultuur is dus ook in dit opzicht erg weerbarstig.

Het vierde cultuurkenmerk dat wij noemden is het proces van sociale categorisatie. Dit is het proces van het onderverdelen van de wereld in *ingroups* en *outgroups*, waarbij de *ingroup* positieve kenmerken krijgt toebedeeld en de *outgroup* negatieve kenmerken. Sociale categorisatie is een barrière tegen de implementatie van IGP omdat het onderlinge concurrentie aanwakkert en leidt tot meer geheimhouding dan noodzakelijk is. Sociale categorisatie is dan ook nauw verbonden met het hierboven beschreven structuurprobleem van de onderlinge concurrentie.

9.3.2 De implementatie van het NIM binnen de CIE

We zullen in deze subsectie bezien in hoeverre de bovengenoemde barrières daadwerkelijk de implementatie van IGP bij de CIE belemmeren. Dit doen we aan de hand van eerder genoemde vijf kenmerken van het NIM (zie subsectie 9.2): (A) de sturing, (B) criminaliteitsanalyse en de opbouw en instandhouding van een informatiepositie, (C) de ontwikkeling naar *need to share*, (D) een adequate ICT-infrastructuur en (E) preventieve voorwaarschuwingen en de bijbehorende proactiviteit naast de traditionele waarheidsvinding en reactieve werkwijze.

A: Sturing

Met betrekking tot de sturing hebben wij geconcludeerd dat dit één van de grote uitdagingen voor de succesvolle implementatie van IGP blijft. Op het moment van schrijven (mei 2012) is er sprake van een soms gebrekkige sturing op strategisch, tactisch en operationeel niveau. Wij zullen het gebrek aan sturing verder toelichten.

Wij hebben met betrekking tot de sturing van de politie geconstateerd dat er weliswaar sprake is van een functionerend stelsel van stuurploegen die strategische beleidsbeslissingen nemen, maar dat dit nog niet leidt tot daadwerkelijke sturing in de zin dat de beslissingen ook daadwerkelijk worden uitgevoerd. Beslissingen worden onvoldoende omgezet in uit te voeren beleid. Daarnaast is het strategisch beleid dusdanig versnipperd dat het uiteindelijk niet effectief is. Bij de CIE wordt er ook gestuurd op de operationele verzameling van informatie, maar wij constateren dat er met name wordt gedebriefd. Van een opdracht in de zin van een briefing is nog te weinig sprake. Dit maakt dat sturing zoals bedoeld binnen IGP nauwelijks plaatsvindt. Wij stellen vast dat de problemen met betrekking tot de sturing grotendeels worden veroorzaakt door een aantal structuurproblemen, en deels door cultuurproblemen.

Twee van de drie de door ons geïdentificeerde structuurproblemen staan een sturing van de politieorganisatie in de weg. Ten eerste is er de traditionele autonome rol van de CIE in het politiebestel. Voor de CIE geldt enerzijds dat zij formeel steeds minder autonoom kan handelen en in toenemende mate ondergeschikt is aan het algemene strategische beleid. In bepaalde gevallen is de CIE zelfs ondergebracht bij de RIO. Anderzijds heeft de CIE echter nog steeds voldoende autonomie om haar eigen koers te varen. Dit komt met name omdat de strategische beslissingen vaag en tegenstrijdig zijn, waardoor er voldoende ruimte is om op de oude manier te werken en toch in lijn met de strategische doelstellingen te werken. Ten tweede is er de feitelijke hiërarchie van de CIE die afwijkt van de formele hiërarchie. De runners hebben bijzonder veel vrijheid bij het inrichten van de eigen werkzaamheden en het is vrijwel ondoenlijk om actief te sturen op de wijze waarop ze de werkzaamheden uitvoeren. De leiding kan hier immers niet bij aanwezig zijn. In die gevallen waarin is geprobeerd om de runners informatie te laten verzamelen op basis van inwinplannen, blijkt dat zij deze betrekkelijk eenvoudig naast zich neer kunnen leggen. Wat overigens niet direct wil zeggen dat zij dat ook daadwerkelijk doen. In de praktijk wordt hier nauwelijks gevolg aan gegeven. De CIE is dus in verregaande mate een *street-level bureaucracy*.

Het belangrijkste cultuurprobleem bij de CIE en de RIO is dat de organisatie wordt geregeerd door de waan van de dag. Dit maakt dat de leidinggevenden primair op gebeurtenissen reageren, maar nauwelijks proactieve, lange-termijn-beslissingen nemen. Ook kunnen veel leidinggevenden het operationele werk moeilijk loslaten, hetgeen ten koste gaat van de lange-termijn-sturing die voor IGP essentieel is.

Wij concluderen al met al dat het voor IGP noodzakelijke vraaggestuurde werken in de praktijk lastig van de grond lijkt te komen.

B: Criminaliteitsanalyse en de opbouw en instandhouding van de informatiepositie

Met betrekking tot criminaliteitsanalyse constateren wij dat deze deels is ingebed in de politieorganisatie. Met name operationele en tactische analyseproducten worden gebruikt bij de besluitvorming, maar slechts in die gevallen waarbij de analist ruimte overlaat aan de leidinggevenden voor de interpretatie. In de gevallen waarin de analist de interpretatie heeft gedaan (hetgeen eigenlijk de kern is van analyse), hebben wij frictie tussen de analisten en de traditionele medewerkers van de politieorganisatie geconstateerd. Met name bij strategische analyses is de ruimte voor interpretatie door anderen dan de analist erg klein. Dit heeft tot gevolg dat de strategische analyse nauwelijks wordt gebruikt bij de effectieve besluitvorming, terwijl het juist deze vorm van op de toekomst gerichte analyse is die zou moeten kunnen leiden tot een daadwerkelijke intelligence-benadering.

Met betrekking tot de criminaliteitsanalyse constateren wij dat de slechte acceptatie met name is terug te voeren op cultuurproblemen. Wij constateren dat er in de praktijk sprake is van een kloof tussen de traditionele recherchefunctie en de nieuwe informatiefunctie. Dit leidt tot onderlinge concurrentie, niet zozeer tussen afdelingen (hetgeen een structuurprobleem is), maar met name tussen de verschillende functionarissen. De kloof speelt dus ook op de werkvloer. Een belangrijke oorzaak hiervoor is de interne sociale categorisatie, waarbij traditionele, executieve politiemensen zich afzetten tegen de hoger opgeleide zij-instromers en andersom. Het gevolg van deze sociale categorisatie is dat het verschil tussen de fase van verzameling van informatie en de fase van analyse van informatie steeds groter wordt. De onderlinge kloof en frictie zorgen ervoor dat het gestructureerde proces wat noodzakelijk is voor het produceren van de intelligence-producten op deze manier niet geïmplementeerd kan worden.

Een ander probleem met betrekking tot de verwerking van informatie en criminaliteitsanalyse is dat de CIE te weinig controlemethoden tot haar beschikking heeft om de betrouwbaarheid van de informant en de informatie te beoordelen. De methoden waarover zij wel beschikt zijn erg arbeidsintensief en tijdsrovend. Daarnaast heeft de CIE nauwelijks controle over deze methoden. Wanneer de betrouwbaarheid van informatie (en informanten) niet kan worden ingeschat, heeft dit belangrijke gevolgen voor criminaliteitsanalyse. Immers, er geldt *rubbish in, rubbish out*. Door de weinige controlemiddelen kan gebrekkige of onjuiste informatie in de analyses worden opgenomen, met als gevolg het risico dat de analyseproducten kwalitatief minder zijn. Dit is geenzins aan de CIE te wijten: zij probeert zoveel mogelijk met de middelen die zij tot haar beschikking heeft tot een betrouwbaarheidsinschatting van de informant en diens informatie te komen. Omdat zij onvoldoende middelen heeft, heeft de CIE voorts onvoldoende zicht op de aard en omvang van het probleem van onbetrouwbare informatie. Wij zijn dan ook van mening dat de bevoegdheden uit de BOB-wetgeving, in bepaalde gevallen en na uitdrukkelijke toestemming door middel van een machtiging van een rechter-commissaris, in de CIE-fase toe te passen zouden moeten zijn ten behoeve van de controle van de informant. Op deze manier is de CIE (en daarmee de rest van de opsporing) veel minder afhankelijk van de informant en is de kans kleiner dat zij ongewild wordt gestuurd. Voor IGP betekent dit dat het zal leiden tot betere informatieproducten.

C: Need to share

Met *need to share* worden twee doelstellingen nagestreefd: (1) het wegnemen van onterechte geheimhouding en (2) het formaliseren van de bestaande informele informatie-uitwisseling (de *old boys networks*). Met betrekking tot het delen van informatie en het *need to share* streven stellen wij vast dat de uitgangspunten van *need to share* binnen CIE worden geaccepteerd en onderschreven. Desondanks is er volgens de heersende collectieve perceptie binnen de rest van de politie sprake van een cultuur van onterechte geheimhouding, en deze cultuur manifesteert zich volgens velen met name bij de CIE. Hiermee zijn veel CIE-ers het (vanzelfsprekend) niet eens. Volgens CIE-ers is men binnen de politie namelijk doorgeschoten met *need to share*, en is het delen van informatie inmiddels een doel op zichzelf geworden. Binnen de CIE wordt aangegeven dat zij inderdaad nog steeds geheimhouding betrachten, maar dat zij dit doen omdat hiervoor een operationele noodzaak bestaat. Daarnaast wijzen zij op het gevaar van CIE-informatie breed ter beschikking te stellen aan anderen die niet op de hoogte zijn van de context van die informatie. Dit zal volgens de CIE al snel kunnen leiden tot verkeerde beslissingen. De verschillende zienswijzen van de CIE en een groot deel van de overige politieorganisatie omtrent de mate van en redenen voor geheimhouding is overigens ook een indicatie voor het hierboven genoemde proces van sociale categorisatie. Binnen de *ingroup* van de CIE sluit men de gelederen tegen de kritiek van buitenaf, hetgeen versterkend werkt voor het 'wij versus zij' gevoel. Dit proces wordt versterkt door de (perceptie van) dwang waarmee *need to share* wordt ingevoerd. Dit leidt niet alleen tot een versterkt saamhorigheidsgevoel binnen de *ingroup* van de CIE, maar mogelijk ook tot actief verzet.

Er wordt geprobeerd om een *free flow* van informatie af te dwingen door de verplichting van bovenaf op te leggen. Dit wordt onder andere gerealiseerd door middel van het wegnemen van technologische barrières tegen het delen van informatie en het ontwikkelen van juridische autorisatiesystemen. Het op deze wijze van bovenaf doorvoeren van *need to share* leidt echter op twee manieren tot verzet binnen de CIE: (1) informatie wordt niet meer in de informatiesystemen ingevoerd en (2) CIE-en wisselen onderling geen informatie meer uit. Het gevolg is dat de algemene informatiepositie van de CIE slechter wordt, hetgeen voor IGP in het algemeen erg slecht zal zijn.

Aan de basis van de barrières tegen het implementeren van *need to share* liggen zowel structuur- als cultuurproblemen. Deze problemen zijn terug te voeren op de institutionele redenen voor geheimhouding en de sociale gevolgen van geheimhouding. De institutionele redenen voor geheimhouding hebben we in sectie 9.1 behandeld. Het gaat om (1) het behoud van invloed, (2) het behoud van autonomie, en (3) een risico-averse mentaliteit. Deze redenen zijn op hun beurt nauw verbonden met concurrentieoverwegingen. Wij zien bij de CIE en de overige onderdelen van de recherche een verregaande onderlinge concurrentie. Met name de komst van de RIO heeft tot concurrentie geleid, omdat de RIO de analysetaak van de CIE op zich heeft genomen. De CIE-en hebben deze taak zelf verwaarloosd door met name te investeren in het verzamelen van informatie en de analysetaak van ondergeschikt belang te achten. Nu de RIO tot taak heeft om inzicht in de zware, georganiseerde criminaliteit en terrorisme te verkrijgen, heeft zij echter ook de CIE-informatie nodig. Immers, zonder deze informatie kan geen volledig beeld worden verkregen. Indien de CIE deze informatie deelt, geeft zij daarmee een deel van haar invloed weg, alsmede haar autonomie. De CIE is dan niet langer degene met de

monopoliepositie op CIE-informatie, maar zij moet dat delen met de RIO. Hierdoor verliest zij een groot deel van haar invloed. Daarnaast raakt de CIE autonomie kwijt, omdat de eigen informatie wordt gebruikt om haar te sturen door middel van het vaststellen van een intelligence-agenda. De CIE gaat dan niet langer zelf over de prioriteiten waar zij zich op richt, maar wordt aangestuurd door anderen. De manier van de CIE om dit te voorkomen, is door informatie niet te delen met de RIO.

De laatste reden is misschien wel de belangrijkste: de operationele reden van geheimhouding. De CIE schermt informatie af om zo de identiteit van de informant geheim te houden. Dit is volgens CIE medewerkers zelf de primaire reden voor geheimhouding. Deze operationele reden voor geheimhouding is legitiem, maar desondanks ook problematisch. Het laat aan de ene kant onverlet dat het in de perceptie van anderen binnen de politieorganisatie wordt misbruikt. Op deze manier ontstaat er een collectief beeld van onterechte geheimhouding die meer te maken heeft met de hierboven genoemde institutionele redenen dan met de operationele redenen. Hier speelt het ongrijpbare van de politiecultuur: er zal in de perceptie van politiemedewerkers die niet bij de CIE werkzaam zijn altijd sprake zijn van onterechte geheimhouding, ongeacht het feit dat de redenen operationeel en dus legitiem zijn. Aan de andere kant biedt de geheimhouding altijd de mogelijkheid om de institutionele redenen voor geheimhouding af te schermen met een zweem van operationele noodzaak. Een dergelijk spookbeeld van onterechte geheimhouding is eigenlijk niet goed te bestrijden, en dit dilemma is dan ook intrinsiek verbonden aan geheimhouding.

Welke van de genoemde redenen het zwaarst wegen, hebben wij niet kunnen vaststellen. Dit is voor ons onderzoek echter ook niet noodzakelijk. Wij constateerden namelijk wel dat in het NIM niet op deze redenen van geheimhouding wordt ingegaan, maar dat het NIM zich richt op het realiseren van bepaalde randvoorwaarden voor het delen van informatie, te weten het slechten van ICT-matige en juridische barrières. Omdat het NIM zich niet richt op het wegnemen van de andere redenen voor geheimhouding, zal geheimhouding altijd aan een volledige implementatie van *need to share* in de weg staan.

Ook met betrekking tot de tweede doelstelling van *need to share,* te weten het formaliseren van de informele informatiestromen, stellen wij vast dat hier nog niet aan is voldaan. De formele informatie- en communicatienetwerken van de politie kennen belangrijke tekortkomingen. Zo is informatie onvindbaar, is er sprake van *data-overload* en is de formele communicatie bewerkelijk en tijdrovend. Om hieraan te ontkomen bestaan er binnen de Nederlandse politie (en de CIE) informele communicatienetwerken: varianten van het *old boys network*. Het NIM probeert aan deze tekortkomingen tegemoet te komen, maar blijkt daarin vooralsnog onsuccesvol. Wij constateren dat het NIM ook met betrekking tot deze tweede doelstelling niet is geslaagd. Dit brengt ons tot onderwerp D: de ICT-infrastructuur.

D: ICT-infrastructuur

De ICT-infrastructuur wordt binnen het NIM gezien als een belangrijke randvoorwaarde voor de implementatie van (de elementen van) IGP, zoals *need to share*. Immers, als de noodzaak tot het delen van informatie wordt onderschreven en de wil is er, dan komt er nog niets van het delen van informatie terecht als de technologie tegenwerkt. Wij hebben echter geconstateerd dat de ICT-systemen bij de politie een zeer hardnekkig structuurprobleem vormen. Dit komt onder meer vanwege de versnippering van de politieorganisatie in het algemeen. Ieder korps (en binnen de

korpsen iedere afdeling) heeft in de afgelopen jaren eigen ICT-systemen ontwikkeld. Inmiddels is er een wirwar van systemen ontstaan die onderling vaak niet goed met elkaar kunnen communiceren. Er is daarom gekozen voor uniforme systemen, maar deze zijn erg verouderd en inefficiënt. Zo zijn ze bijzonder gebruikersonvriendelijk en verdwijnt er veel informatie in het systeem. Een versnipperde informatiepositie is het gevolg. Omdat IGP met name uitgaat van de productbenadering van intelligence, waarbij data aan de basis ligt van de informatie- en intelligenceproducten, werken deze systeemproblemen verlammend op de implementatie van het gehele concept.

E: Voorwaarschuwingen en proactiviteit

Als laatste behandelen wij het gebruik van voorwaarschuwingen en de daarbij behorende proactieve werkwijze. Wij stelden vast dat de voorwaarschuwingsfunctie van intelligence niet expliciet als een onderdeel van IGP wordt benoemd. Het volgt echter wel uit de breed uitgesproken wens om criminaliteit meer te voorkomen en 'meer aan de voorkant te zitten'. In de praktijk constateerden wij echter ook dat er van een uitwerking van de voorwaarschuwingsfunctie weinig terecht komt. Dit heeft onder andere te maken met het hiervoor behandelde gegeven dat de strategische criminaliteitsanalyse een veel te marginale rol heeft binnen de politieorganisatie. Zoals gezegd is het juist deze strategische analyse die een meerwaarde heeft binnen het intelligence-proces.

Wij stelden vast dat de CIE nog steeds in hoge mate reactief werkt. Een proactieve werkwijze wordt niet bereikt omdat de CIE (1) afhankelijk is van informanten, (2) afhankelijk is van tactische opsporingsteams en (3) nauwelijks gebruik maakt van technologische innovaties. Veel informatieverzameling door de CIE wordt nog steeds geleid door de waan van de dag. Deze afhankelijkheid van andere partijen voor informatievoorziening gecombineerd met een conservatieve houding ten opzichte van nieuwe technologieën maakt dat de CIE anno 2012 niet proactief in de zin van IGP is.

Dat de CIE niet aan voorwaarschuwingen doet en reactief werkt, heeft deels te maken met de weerbarstige cultuur. Wij constateerden dat met name een conservatieve houding ten opzichte van alle soorten van veranderingen (inclusief IGP) ervoor zorgt dat de CIE achterblijft bij deze ontwikkelingen. Andere afdelingen zoals de RIO's lijken in de ogen van de CIE wel steeds meer de IGP-kant op te gaan, hetgeen een aparte dynamiek krijgt in het proces van sociale categorisatie. Die andere afdelingen zijn in een zeker opzicht concurrenten van de CIE en veel kenmerken van die concurrenten zullen als negatief worden bestempeld. Het betreft immers een *outgroup*. Ook het vasthouden aan de reactieve, waan-van-de-dag- mentaliteit kan worden verklaard met de conservatieve houding. Wij merken echter ook op dat het politiewerk altijd deels reactief zal moeten blijven: de opsporing en bijbehorende waarheidsvinding blijven nog steeds een taak van de politie in het algemeen en de CIE in het bijzonder. Hier kan niet altijd aan worden ontkomen.

9.3.3 Concluderend

Al met al stellen wij vast dat er in hoofdlijnen van IGP binnen de CIE nog nauwelijks sprake is. De gewenste paradigmawijziging heeft zich niet vertaald naar een verandering in de CIE-praktijk, en de CIE werkt nog grotendeels op dezelfde, traditionele wijze als voor de komst van IGP. Dit is echter niet echt verwonderlijk:

een paradigmawijziging is niet van het ene op het andere moment gerealiseerd en vergt bijzonder veel tijd en inspanningen.

9.4 De verhouding tussen de AIVD en de CIE

In deze sectie beantwoorden wij de vierde onderzoeksvraag OV 4. Deze luidt als volgt.

Wat is de verhouding tussen de AIVD en de CIE in de praktijk?

Wij gaan bij het beantwoorden van deze vraag allereerst in op de verschuiving in de traditionele conceptuele verhouding tussen de veiligheidsdiensten (subsectie 9.4.1). Vervolgens behandelen wij de interactie tussen de AIVD en de CIE en de rol van vertrouwen in de onderlinge relatie tussen de AIVD en de CIE (subsectie 9.4.2). Daarna gaan wij in op de wijze waarop de verhouding in de praktijk vorm krijgt (subsectie 9.4.3).

9.4.1 Verschuivingen in de conceptuele verhouding

De traditionele verhouding tussen de veiligheidsdienst en de politie in het algemeen isanno 2012 niet meer van toepassing. Wij constateerden belangrijke verschuivingen bij de kenmerken van de politie die in toenemende mate gelijke kenmerken krijgt als de veiligheidsdienst. Deze veranderingen zullen we hier kort weergeven.

Met betrekking tot het eerste kenmerk (A: de taakstelling) stelden wij vast dat hier *in abstracto* geen veranderingen zijn opgetreden: de politie is nog steeds belast met de strafrechtelijke handhaving van de rechtsorde. Wij constateren echter wel een verandering in de concrete invulling van de taak. Steeds meer gedragingen zijn onder het bereik van het strafrecht gekomen en behoren daarmee tot de taak van de politie. Sinds 11 september 2001 en de daaropvolgende nieuwe wetgeving heeft de politie formeel juridisch ook een belangrijke rol gekregen bij de bestrijding van terrorisme. De bestrijding van terrorisme was sinds de jaren ‘90 exclusief voorbehouden aan de AIVD (toen nog BVD geheten), maar dat veranderde aldus in 2001. De politie heeft sinds 2001 nieuwe bevoegdheden gekregen die het haar mogelijk maken om in een vroeg stadium onderzoek te doen naar terrorisme. In dit opzicht vertoont het aandachtsgebied waar de politie zich op richt belangrijke gelijkenis met die van de veiligheidsdiensten. Het gevolg hiervan is dat de AIVD en de politie elkaar in toenemende mate in operationele *settings* zullen tegenkomen.

Wij stelden vast dat terrorismebestrijding bij de CIE moeilijk uit de verf komt. Het is een relatief nieuw onderwerp zonder de ‘dynamiek’ en spanning van het traditionele politiewerk. Verder bestaat bij de politie in het algemeen de neiging om alle vormen van criminaliteit waarin sprake is van een ideologische component onder de noemer ‘terrorisme’ te scharen. Terrorisme bij de politie bestaat voorts uit veel verschillende elementen waarin de onderlinge samenhang ontbreekt (zoals links extremisme, Turks nationalisme en jihadistisch terrorisme). Het onderwerp terrorisme vereist andere en meer diverse kennis en competenties van de betrokken CIE-medewerkers, zoals kennis van de islam en kennis van extreem-links. Er zijn niet veel politiemedewerkers die over de vereiste kennis en competenties beschikken en veel medewerkers stappen naar verloop van tijd over naar andere aandachtsgebieden. Ondanks de hiervoor beschreven moeilijkheden met betrekking tot het onderwerp terrorisme, stellen wij ook vast dat de CIE en de AIVD elkaar in toenemende mate in

lopende onderzoeken zijn tegengekomen en tegenkomen. Dit vereist meer onderlinge afstemming, informatie-uitwisseling en operationele samenwerking.

Met betrekking tot (B) het middel waarmee de organisaties proberen de taak te vervullen zien wij ook belangrijke verschuivingen. Van de politie wordt in toenemende mate verwacht dat zij naast de waarheidsvinding ook voorwaarschuwingen gaat geven. Dit betekent dat het opbouwen en in stand houden van een informatiepositie een veel grotere rol krijgt dan voorheen.

Het genereren van voorwaarschuwingen stelt andere eisen aan de wijze waarop de politie omgaat met informatie, hetgeen de reden is voor de politie om een ander werkproces te adopteren: (C) de intelligence cyclus. Deze cyclus wijkt in belangrijke mate af van het opsporingsproces omdat het meer gestructureerd is en uitgaat van specialisatie per fase. Dit geldt met name voor de fase van analyse.

Met betrekking tot het laatste kenmerk (D: relatie externen) stellen wij vast dat de politie hier een tegengestelde ontwikkeling lijkt door te maken: onder de noemer van *need to share* wordt binnen politie gestreefd naar meer interne transparantie. Het idee is dat informatie gedeeld moet worden om zo tot betere intelligenceproducten te komen. In eerste instantie lijkt de politie hiermee nog verder van de veiligheidsdienst te bewegen.

Al met al concluderen wij dat de veiligheidsdiensten en de politie in theorie steeds meer gelijke kenmerken krijgen. Schematisch ziet de ontwikkeling er als geschetst in figuur 9.1 (eveneens geleend van figuur 8.2) uit.

Dienst	**AIVD (HP)**	**Politie (LP)**
Taak	Nationale Veiligheid: Terrorisme, gewelddadig (politiek) activisme	Rechtsorde: Criminaliteit + *ideologische misdrijven*
Middel	Voorwaarschuwing: Opbouw & instandhouding informatiepositie	Waarheidsvinding: verzamelen bewijs + *voorwaarschuwing / opbouw & instandhouding informatiepositie*
Werkproces	Intelligence-cyclus	Opsporing + *intelligence-cyclus*
Relatie externen	Geheimhouding	Transparantie

Figuur 9.1: veranderingen in de verhouding

9.4.2 De interactie en de rol van vertrouwen

Nu de diensten zich op hetzelfde aandachtsgebied richten, dezelfde doelstelling nastreven en op dezelfde wijze lijken te gaan werken, zullen ze elkaar ook steeds vaker tegenkomen. Dit leidt tot de noodzaak om (1) activiteiten onderling op elkaar af te stemmen, (2) informatie te delen en (3) in bepaalde gevallen zelfs samen te werken. Deze drie elementen van interactie staan op volgorde van de mate van vertrouwen dat nodig is tussen de organisaties. Wij constateerden dat dit vertrouwen in de praktijk echter zeer problematisch is. Hiertoe hebben wij vertrouwen eerst conceptueel benaderd en dit concept hebben wij vervolgens toegepast op de situatie tussen de AIVD en de politie.

Wij stelden vast dat vertrouwen uit drie elementen bestaat: (1) er is een relatie tussen A, B en X die niet hiërarchisch van aard is, (2) er is een reden (*incentive*) om te

vertrouwen en (3) er bestaat een risico dat het vertrouwen wordt beschaamd. Dat de beide organisaties een reden (*incentive*) hebben om elkaar te vertrouwen volgt uit de hierboven geschetste conceptuele ontwikkelingen en de mogelijke implicaties voor de praktijk van de terrorismebestrijding. Het is immers denkbaar dat de politie in een vroeg stadium AIVD-agenten in beeld krijgt, een opsporingsonderzoek opstart en op deze manier de inlichtingentrajecten van de AIVD doorkruist. Dit is voor beide diensten onwenselijk. De eerste reden verdient echter een nadere toelichting.

Op het eerste gezicht lijken de AIVD en de CIE formeel in een functionele hiërarchische relatie tot elkaar te staan. Zo heeft de AIVD op basis van artikel 38 WIV 2002 een discretionaire bevoegdheid om informatie te verstrekken aan de politie, maar heeft de politie op basis van artikel 62 WIV 2002 de plicht om informatie aan de AIVD te verstrekken indien deze dat nodig heeft voor een goede uitvoering van zijn taak. De politie maakt zelf echter de afweging of de informatie van belang is voor de uitvoering van de AIVD-taak en, belangrijker, bepaalt zelf het tijdstip van daadwerkelijke verstrekking. Dit geldt met name voor de gevoelige CIE-informatie. In de WPG is een bepaling opgenomen (artikel 24) die de beoordelingsruimte voor de politie kleiner moet maken, maar dit geldt vooralsnog niet voor de gevoeligste CIE-informatie. Zelfs als ook de formeel juridische mogelijkheden van de CIE om informatie voor de AIVD af te schermen worden weggenomen, bestaat er nog de mogelijkheid dat de CIE-medewerkers bepaalde informatie niet in het systeem opslaan of onder een hogere afschermingscodering wegschrijven dan strikt genomen noodzakelijk is. In de praktijk is er dus geen sprake van een materiële hiërarchische relatie tussen de AIVD en de CIE: de AIVD kan de CIE niet dwingen om informatie te verstrekken.

De reden waarom het moeilijk is om tot een situatie van vertrouwen te komen, ligt in het derde kenmerk: het risico. De verregaande geheimhouding aan de kant van de AIVD en de transparantie aan de kant van de politie maken het risico van een mogelijk geschaad vertrouwen groot. De CIE kan er niet op vertrouwen dat de AIVD haar belangen behartigt omdat zij dit, vanwege de geheimhouding, eenvoudigweg niet kan inschatten. Geheimhouding leidt vrijwel automatisch tot negatieve beeldvorming, hetgeen het vertrouwen negatief beïnvloedt. Voor de AIVD geldt dat aan de politie verstrekte informatie met teveel mensen kan worden gedeeld, zeker indien er volgens het *need to share* denken wordt gehandeld. Dit en de 'tirannieke werking van het procesdossier' maakt dat de AIVD de politie niet kan vertrouwen omdat het risico te groot is dat het vertrouwen wordt geschonden.

Omdat het risico te groot is, zal er niet snel sprake zijn van vertrouwen tussen de AIVD en de CIE. In de volgende subsectie bezien we tot welke interactie in de praktijk wordt overgegaan en in hoeverre de vertrouwensrelatie daar een rol speelt.

9.4.3 De interactie in de praktijk

Met betrekking tot de eerste modaliteit van interactie, de onderlinge afstemming van werkzaamheden, constateerden wij dat deze in de praktijk redelijk tot goed verloopt. In de overleggen van het IOT en het AOT worden activiteiten afgestemd, en de betrokkenen zijn positief over de samenwerking. Bij deze interactie behouden beide partijen hun invloed en autonomie, hetgeen het delen van informatie gemakkelijker maakt. Daarnaast zijn de overleggen kleinschalig, waardoor de aanwezigen sneller een persoonlijke inschatting kunnen maken over met wie ze informatie delen. Er is met andere woorden weinig anonimiteit.

Met betrekking tot de tweede modaliteit van interactie, de informatie-uitwisseling, stelden we echter vast dat deze minder goed verloopt. Hier speelt het element van risico sterker dan bij het afstemmingsoverleg. Vanuit de CIE is er terughoudendheid met betrekking tot het delen van de 00, 200 en 300 informatie met de AIVD omdat dit tot niet in te schatten veiligheidsrisico's leidt. De informatie wordt aan een anonieme partij verstrekt, te weten de AIVD, en wat er verder met de informatie gebeurt, is niet in te schatten. De AIVD verstrekt op zijn beurt nog steeds vrijwel geen informatie aan de CIE: hiertoe zou de WIV 2002 geen mogelijkheden bieden. In hoeverre de angst voor het verlies van invloed en autonomie bij de AIVD een rol speelt, konden wij overigens niet beoordelen.

Omdat de laatste modaliteit van interactie, te weten de onderlinge samenwerking, de meeste openheid en vertrouwen over en weer vergt, is dit de meest problematische modaliteit. Met name de AIVD is terughoudend met daadwerkelijke samenwerking. De CT-infobox is een verregaande poging tot samenwerking, maar wij constateren dat vanuit het oogpunt van samenwerking de CT-infobox niet goed werkt. De CT-infobox valt onder verantwoordelijkheid en aansturing van de AIVD, en is zelfs in het pand van de AIVD gevestigd. Voor politiemensen zijn de CT-infobox en de AIVD hetzelfde. Dit is dan ook geen echte samenwerking. Er zou van een daadwerkelijke samenwerking sprake kunnen zijn indien er meer sprake is van gelijkwaardigheid en de betrokken partijen niet meer vallen onder verantwoordelijkheid en aansturing van de AIVD. Hiermee is overigens niet gezegd dat er thans geen werkbare situatie is.

Al met al constateren wij dat de AIVD en de CIE (en de politie in het algemeen) nog steeds gescheiden van elkaar zijn er er dus weinig sprake is van structurele informatie-uitwisseling of samenwerking. Pas wanneer er aan alle voorwaarden voor vertrouwen wordt voldaan, kan er daadwerkelijk gewerkt worden aan interactie die verder gaat dan afstemming en marginale informatie-uitwisseling.

9.5 Antwoord op de centrale probleemstelling

De resultaten van ons onderzoek zoals weergegeven in dit proefschrift geven een antwoord op centrale probleemstelling. De probleemstelling luidt als volgt.

Wat zijn de gevolgen van de implementatie van het concept van intelligence in de context van de Nederlandse opsporing voor de verhouding tussen de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Criminele Inlichtingeneenheid (CIE) van de Nederlandse politie?

Het is nu zaak om de antwoorden op de onderzoeksvragen met elkaar te verbinden om zo een antwoord te geven op de centrale probleemstelling. Wij behandelen daartoe allereerst in subsectie 9.5.1 in hoeverre er een verschuiving plaatsvindt. Vervolgens behandelen we in subsectie 9.5.2 of er een causaal verband bestaat tussen de invoering van IGP in de context van de CIE en de verhouding tussen de CIE en de AIVD.

9.5.1 Verschuivingen in de verhouding?

We hebben vastgesteld dat er in theorie verschuivingen plaatsvinden in de kenmerken van de politie. De politie, en daarmee ook de CIE, vertoont in toenemende mate gelijkenissen met de veiligheidsdiensten. Voor een groot deel betreft dit echter de

conceptuele verhouding (de veranderende kenmerken van de politie en CIE zoals het op papier in wetgeving, visiedocumenten en beleidsstukken wordt voorgesteld) en niet de politiepraktijk. Wij stellen dan ook vast dat de veranderingen in de praktijk veel minder ver gaan dan wordt beoogd. Alhoewel de CIE een steeds grotere rol heeft gekregen bij de bestrijding van terrorisme, vervult zij deze taak grotendeels op dezelfde wijze als waarop ze altijd heeft gewerkt: als een reactieve organisatie die de tactische opsporing ondersteunt door middel van het verzamelen van informatie en het runnen van informanten. Van een stelselmatig gebruik van voorwaarschuwingen is geen sprake, en de opbouw en instandhouding van de informatiepositie zijn primair gericht op het ondersteunen van de waarheidsvinding. Ook de implementatie van een gestructureerd en vraaggestuurd werkproces komt in de praktijk nauwelijks van de grond. Daarnaast houdt de CIE nog steeds vast aan de (operationele) geheimhouding die zij betracht ten behoeve van de afscherming van de identiteit van de informant. Al met al is er van een daadwerkelijke verschuiving van de CIE in de richting van een veiligheidsdienst dus geen sprake.

Een verhouding omvat echter meer dan de vraag in hoeverre de organisaties verschillende kenmerken hebben. Het gaat ook om de wijze waarop de organisaties interactie met elkaar hebben. Hierin zien wij wel wat meer verschuivingen. De AIVD en de CIE komen elkaar in de praktijk steeds vaker tegen. Want ondanks dat de CIE grotendeels op dezelfde wijze blijft werken, zijn de onderwerpen waar zij zich op richt wel aanzienlijk uitgebreid. De CIE richt zich tegenwoordig ook op de bestrijding van terrorisme (in het jargon ook wel 'ideologische misdrijven' genoemd). Ofschoon de extra capaciteit die op terrorismebestrijding wordt ingezet niet bijzonder groot is, bestaat er wel altijd het risico dat de AIVD en de CIE in dezelfde vijver vissen en elkaars trajecten doorkruisen. Vanuit beide organisaties vloeit hieruit een noodzaak tot afstemming, informatie-uitwisseling en samenwerking voort. Immers, het is denkbaar dat de CIE informanten runt in een netwerk waarin ook de AIVD agenten en informanten heeft zitten, met als risico dat bijvoorbeeld informatie wordt gedubbeld. Daarnaast is er altijd het risico dat de politie in een vroeg stadium overgaat tot verstoring of aanhouding van terroristische netwerken, terwijl de AIVD daar nog inlichtingenbelangen heeft. Zonder een bepaalde mate van afstemming, informatie-uitwisseling en samenwerking is het risico aanwezig dat de organisaties elkaar meer in de weg zitten dan dat ze elkaar helpen. De verhoogde noodzaak tot onderlinge interactie leidt echter slechts in beperkte mate tot daadwerkelijke interactie. Dit komt met name omdat het onderlinge vertrouwen in de praktijk wordt belemmerd door geheimhouding over en weer. De geheimhouding is weer terug te voeren op een zekere mate van concurrentiestrijd tussen beide organisaties met als inzet invloed en autonomie. De diensten komen in dit opzicht ook van ver. Er heeft altijd een verregaande scheiding tussen de AIVD en de politie bestaan, en deze is niet van de ene op de andere dag weggenomen.

De AIVD en de politie staan in een complexe verhouding tot elkaar. Het zijn van elkaar gescheiden organisaties die worden gedwongen om meer toenadering tot elkaar te zoeken, terwijl de verhouding meer kenmerken heeft van concurrentie. Het blijkt erg moeilijk te komen tot een onderling vertrouwen en een structurele afstemming van activiteiten, informatie-uitwisseling of samenwerking. Wij hebben echter ook vastgesteld dat alhoewel de implementatie van IGP ertoe leidt dat de AIVD en de CIE steeds meer gelijkenissen zullen gaan vertonen, de daadwerkelijke implementatie van IGP in de praktijk helemaal niet spoedig verloopt. In de kern blijven de AIVD en de CIE dus verschillende organisaties met elk een eigen taak, doelstelling en werkmethoden. Hierdoor zullen de veranderingen in de verhouding in

de praktijk veel minder ver gaan dan op basis van de theorie in eerste instantie het geval lijkt te zijn.

9.5.2 Causaal verband?

Het bovenstaande roept de vraag op naar een causaal verband tussen (1) de implementatie van IGP en (2) de conceptuele verschuivingen en de verschuivingen in de praktijk. De vraag wanneer zaken in een causale relatie tot elkaar staan, is in de sociale wetenschappen echter zeer moeilijk te beantwoorden. Er zijn immers heel veel mogelijke variabelen die een rol spelen, en het is afhankelijk van het gekozen perspectief van de betreffende onderzoeker welke variabelen een causaal verband met een gebeurtenis krijgen toegedicht.

Welke variabelen worden benoemd, hangt ook af van het niveau van de analyse. Wanneer de verhouding tussen de AIVD en de CIE op het niveau van de individuele medewerker wordt bekeken, biedt de psychologie wellicht een betere verklaring voor de verhouding dan theoretische modellen die zien op de relatie tussen organisaties. Omdat wij geen psychologen zijn, hebben wij dit individuele niveau nauwelijks behandeld. Wij zijn ons er echter wel van bewust dat in ons onderzoek verschillende analyseniveaus door elkaar heen lopen. Het is ons doel om de complexiteit van een verandering als IGP te schetsen, en deze complexiteit kan alleen worden begrepen wanneer de verschillende niveaus worden meegenomen in de analyse. Wij constateren ook dat de niveaus niet los van elkaar staan, maar een voortdurende invloed uitoefenen op elkaar. Dit speelt een belangrijke rol bij het vaststellen van causaliteit. Daarnaast hebben wij een exploratief onderzoek uitgevoerd, waarbij we niet de pretentie hebben om voor alles wat wij hebben waargenomen een passend of bevredigend antwoord te hebben. Wij zullen de vraag naar de causaliteit beantwoorden aan de hand van de door ons gebruikte definitie van IGP.

Binnen de politie wordt IGP met name gezien als een gestructureerd werkproces, waarbij politieactiviteiten worden gestuurd op basis van geanalyseerde informatie. Indien deze zienswijze wordt gehanteerd, is er nauwelijks sprake van een causaal verband tussen de verschuivingen in de LP-kenmerken van de CIE naar HP-kenmerken en de implementatie van IGP. De verschuivingen vinden wel plaats, maar moeten los worden gezien van IGP. Wij hanteren echter een andere definitie van IGP die niet alleen meer recht doet aan de achterliggende redenen waarom de politie volgens IGP wil werken, maar die ook meer causaal verband laat zien in de veranderende verhouding tussen de veiligheidsdiensten en de politie op de verschillende niveaus. IGP is namelijk de implementatie van het concept van intelligence in de context van de politie (en dus de CIE). Intelligence hebben wij (kort samengevat) gedefinieerd als een concept waarbij door middel van de intelligence-cyclus gekomen wordt tot voorwaarschuwingen die preventieve acties mogelijk maken. Het gaat dan niet alleen om die gestructureerde, vraaggestuurde intelligence-cyclus, maar ook wat daarmee wordt beoogd, te weten het geven van voorwaarschuwingen. Wanneer we de verschuivingen vanuit dat perspectief bezien, stellen we vast dat veranderingen in middel, werkconcept en relatie met externen in potentie worden beïnvloed door IGP. IGP beoogt de politie op al deze elementen te veranderen. Het causale verband tussen IGP en de veranderende verhouding ligt in het feit dat IGP het conceptuele raamwerk is waarin de veranderende verhouding vorm krijgt. De veranderingen in de taakstelling en het aandachtsgebied staan in zoverre grotendeels los van IGP dat deze niet direct door IGP worden veroorzaakt. Er is

echter wel een verband tussen beide. Wij constateren dat de uitbreiding van het aandachtsgebied van de politie met terrorismebestrijding een stimulans is voor de implementatie van IGP. Terrorismebestrijding leent zich immers bij uitstek voor een intelligence-benadering omdat terroristische aanslagen voorkomen moeten worden. Opsporing en waarheidsvinding is hier van minder groot belang.

Naast een causaal verband tussen de hierboven geschetste conceptuele verhouding stellen wij ook vast dat IGP van invloed is op de interactie tussen veiligheidsdiensten en de politie in het algemeen en tussen de AIVD en de CIE in het bijzonder. IGP vormt het referentiekader van de politie; het is in een zeker opzicht de bril waardoor zij naar de werkelijkheid kijkt. Een onderdeel van die werkelijkheid is de verhouding met de AIVD. De vertrouwensrelatie tussen de organisaties krijgt door IGP dan ook een andere dynamiek. IGP verandert één van de organisaties in die verhouding en daarmee de verhouding op zich. Zo worden de opbouw en de instandhouding van de politiële informatiepositie door IGP steeds belangrijker. In zekere zin wordt de politie net als de AIVD in toenemende mate gekenmerkt door een soort informatie-absorptieproces, waarbij de AIVD verder ook wordt gezien als een potentiële informatiebron. Dus is de AIVD naast een afnemer van informatie ook een potentiële bron van informatie. Dit verandert de interactie tussen de organisaties: de politie zal zich anders moeten opstellen wil zij informatie van de AIVD krijgen (voor zover dit juridisch gezien al mogelijk zou zijn). Daarnaast is het ook niet ondenkbaar dat wanneer de AIVD en de politie beide volgens het concept van intelligence werken en zij zich op dezelfde onderwerpen richten, de onderlinge concurrentie juist zal toenemen in plaats van afnemen. Immers, de AIVD en de CIE mogen dan wel vergelijkbare kenmerken hebben, ze blijven verschillende organisaties met elk hun eigen belangen. Daar waar de informatieproducten van de AIVD en de CIE voorheen duidelijke verschillend waren, zal dat verschil kleiner worden als de CIE volgens IGP gaat werken. De CIE zal bij IGP immers ook intelligenceproducten opleveren. Indien verschillende organisaties dezelfde producten opleveren, is concurrentie doorgaans een logische consequentie.

9.6 Discussie

Een exploratief onderzoek zoals dat van ons roept op zijn minst evenveel vragen op als dat het antwoorden geeft. In deze studie geven wij een aanzet tot een verdere discussie omtrent IGP en de verhouding tussen de AIVD en de politie. De door ons geformuleerde antwoorden op de probleemstelling roepen allereerst de vraag op of, en zo ja, hoe men binnen de politie verder moet gaan met de implementatie van IGP. De tweede vraag die rijst is op welke wijze de verhouding tussen de AIVD en de CIE kan worden verbeterd. Wij behandelen in subsectie 9.6.1 de eerste vraag aan de hand van de geconstateerde barrières die de implementatie van IGP in de weg staan. Vervolgens behandelen we in subsectie 9.6.2 de verhouding tussen de AIVD en de CIE aan de hand van de barrières die het vertrouwen tussen de organisaties in de praktijk in de weg staan. Een discussie met als onderwerp de politie kan anno 2012 overigens niet worden gevoerd zonder stil te staan bij de nog te vormen nationale politie.[298] Daarom zullen we zowel in 9.6.1 als 9.6.2 kort stilstaan bij de mogelijke impact die de nog te vormen nationale politie kan hebben op onze constateringen.

[298] Op 1 januari 2012 zou het er eindelijk van moeten zijn gekomen: een nationale politie. Het betreft de grootste reorganisatie van het politiebestel die Nederland ooit heeft gezien, van 26 korpsen naar 11 districten en een landelijke eenheid. En ook de districten zouden vergelijkbaar worden ingericht, met elk een RIO, zogenoemde 'robuuste basiseenheden', die geacht worden de uiteenlopende politietaken

9.6.1 De barrières tegen IGP

Wij beginnen de discussie met betrekking tot IGP met een algemene discussie waar volgens ons in de politiepraktijk aan voorbij is gegaan: (A) de vraag of IGP wenselijk is. Vervolgens behandelen wij de barrières die een succesvolle implementatie van IGP in de weg staan, te weten (B) de onduidelijkheid omtrent IGP, (C) de hardnekkige structuurkenmerken, en (D) de weerbarstige politiecultuur.

A: De wenselijkheid van IGP

De discussie naar de wenselijkheid van een ontwikkeling als IGP is eigenlijk van het hoogste belang. Binnen de politieorganisatie wordt het concept door beleidsmakers omarmd en de implementatie ervan vindt plaats zonder een uitgesproken discussie omtrent de wenselijkheid. De praktijk van IGP laat echter zien dat de implementatie niet zonder slag of stoot plaatsvindt. Er is kennelijk weerstand tegen de implementatie van het concept. De vraag is dan ook of het wenselijk is dat de politie IGP als uitgangspunt neemt. Is het nodig dat de politie een paradigmawijziging doorvoert en, zo ja, waarom is intelligence dan het aangewezen concept? En vereist intelligence niet teveel veranderingen van de politie?

Wij constateren dat er nog nauwelijks empirisch bewijs bestaat waaruit blijkt dat IGP leidt tot betere resultaten dan de traditionele werkwijzen. Vooralsnog gaat het om aannames. Wij pleiten er daarom voor dat de politie zich heroriënteert op haar kerntaken en meer uitgaat van haar eigen toegevoegde waarde als het gaat om de algemene veiligheidszorg. Met betrekking tot criminaliteitsbestrijding zijn dat de opsporing en de strafrechtelijke waarheidsvinding. Daartoe beschikt de politie over wettelijke bevoegdheden die andere instanties eenvoudigweg niet hebben, en daarin ligt onzes inziens in belangrijke mate de kracht van de politieorganisatie. Dit laat onverlet dat de politie oog zal moeten hebben voor trends en ontwikkelingen op het gebied van de zware georganiseerde criminaliteit en dat het werkproces meer gestructureerd moet plaatsvinden. Maar de vraag is of een gehele paradigmawijziging noodzakelijk is om de gewenste resultaten te bereiken, of dat de politie beter gericht op een klein aantal aspecten van de organisatie en werkwijze bepaalde veranderingen kan doorvoeren. Zo zou het ook mogelijk kunnen zijn dat de politie meer volgens een netwerkbenadering gaat werken en bepaalde specialistische kennis op ad hoc basis inhuurt. Voor het beschrijven van CBA's kunnen bijvoorbeeld ook universiteiten worden benaderd. De vraag of het verstandig is dat de politie alle kennis zelf in huis moet hebben en de gehele organisatie moet worden gereorganiseerd waarbij eigenlijk wordt gegokt op een goede uitkomst, kunnen wij echter niet beantwoorden. Het is mogelijk dat IGP, wanneer het goed wordt geïmplementeerd, daadwerkelijk tot goede resultaten leidt. Wij stellen alleen vast dat de aannames waarop IGP wordt gebaseerd, hoewel in zekere zin logisch en verklaarbaar, nog een empirische onderbouwing missen. Daarnaast zijn wij ons ervan bewust dat de beweging die de politie heeft ingezet om verschillende redenen niet meer te stoppen is en dat een discussie in deze

---

te kunnen vervullen, en landelijk vastgestelde prioriteiten. Het wachten is nog op de komst van de nieuwe politiewet, die de reorganisatie mogelijk maakt. De oprichting per 1 januari 2012 is niet gehaald. De Eerste Kamer wil het voorstel goed behandelen, en niet als het 'hamerstuk' wat de minister ervan maakt. En ook de Tweede Kamer heeft besloten dat zij meer tijd nodig heeft voor een inhoudelijke behandeling van de wet. De reorganisatie is dan ook voor een nog onbepaalde tijd uitgesteld. Maar dat er uiteindelijk een nationale politie aankomt lijkt onafwendbaar.

fase te laat komt. Aangenomen dat dit zo is, dan hebben wij nog een aantal andere punten waarover volgens ons beter nagedacht en gediscussieerd mag worden.

B: De onduidelijkheid omtrent IGP

De onduidelijkheid omtrent de betekenis van het begrip IGP en de verschillende elementen staat een goede implementatie in de weg. Wij zijn echter van mening dat dit probleem in de praktijk niet gemakkelijk op te lossen is. De term is inmiddels verworden tot een modeterm welke te pas en te onpas wordt gebruikt voor verschillende ontwikkelingen. Alhoewel er een doctrine IGP is (zie Kop en Klerks 2009), lijkt deze niet te zijn doorgedrongen tot de werkvloer. Dit komt ook door de versnippering binnen de politie: er zijn zoveel organisatieafdelingen waar iets met IGP wordt gedaan, dat het inmiddels is verworden tot een recept voor alle kwalen. Een zekere mate van ambiguïteit met betrekking tot de term IGP behoeft de implementatie ervan niet in de weg te staan, maar dit geldt met name voor de fase waarin de agenda voor de beoogde verandering wordt vastgesteld. In die fase is het goed om met een ambigu begrip te werken, omdat het de verschillende actoren kan verzamelen rond het concept IGP. Bij de implementatie van IGP is het echter verstandig om het concept te operationaliseren in concrete, uitvoerbare plannen. Wij voegen hieraan toe dat dit van de plannen vereist dat ze begrijpelijk zijn en aansluiten op de concrete problemen waarvoor de verandering een oplossing biedt. De producten van ABRIO en het NIM bieden hiervoor een goede eerste aanzet, maar het is nu de noodzaak ze zo om te vormen dat ze helder, concreet en goed te implementeren zijn.

De vraag is nu in hoeverre de nationale politie invloed op de onduidelijkheid van IGP zal hebben. Hierover kunnen we kort zijn. Het is niet te verwachten dat men in het kader van de voorgenomen reorganisatie zal komen met een duidelijke uniforme formulering van IGP die vervolgens daadwerkelijk wordt uitgedragen en gestructureerd wordt ingevoerd. De reorganisatie is daar niet op gericht. Voor IGP is de uniforme en prominente die de RIO's binnen de nationale politie zullen krijgen in het algemene informatieproces wel bijzonder relevant. Over de RIO's valt namelijk het volgende te lezen: "*De DRIO is verantwoordelijk voor het overzicht op en inzicht in de regionale en lokale veiligheidssituatie en draagt zodoende bij aan de sturing op het politiewerk. Daartoe legt de DRIO zich toe op het verzamelen, inwinnen, ontsluiten, veredelen, analyseren, coördineren, verstrekken, verwerken en beheren van informatie*" (Ontwerpplan National Politie 2011: 41).[299] Het zal duidelijk zijn dan de RIO de primaire verantwoordelijkheid heeft over het implementeren van IGP, en indien de RIO's allemaal vergelijkbaar gaan werken, zal dit de duidelijkheid omtrent IGP alleen maar ten goede komen.[300]

[299] Tussen onze terminologie en de terminologie die binnen de nationale politie wordt gehanteerd zit soms een klein verschil. Zo spreekt het ontwerpplan van de Dienst Regionale Informatie Organisatie, oftewel DRIO waar wij de op het moment gebruikelijke term RIO hanteren. Inhoudelijk verschillen deze begrippen niet van elkaar.

[300] De invulling en uitvoering van de reorganisatie is weliswaar op hoofdlijnen uitgekristalliseerd, op detailniveau laat zij echter nog wel te wensen over. Dit is iets waar men binnen de CIE ook last van heeft of gaat hebben. Zo is het onduidelijk wat er met veel leidinggevenden inclusief het hoofd CIE gaat gebeuren. Immers, wanneer men van 26 naar 11 CIE-en gaat, blijven er 15 hoofden CIE over. Dit geldt overigens ook voor overige rechercheafdelingen. Deze details zijn de oorzaak van veel onzekerheid op de werkvloer. Omdat dit verder geen raakvlakken met IGP heeft, laten wij dit verder buiten beschouwing.

C: De hardnekkige structuurkenmerken

Voor de duidelijkheid herhalen we hier de hardnekkige structuurkenmerken die we in subsectie 9.3.1 hebben geformuleerd. Het gaat om: (1) een grote fragmentatie binnen de politieorganisatie, waardoor autonome machtsblokken zijn ontstaan, (2) onderlinge concurrentie tussen de verschillende afdelingen binnen de politie en (3) een feitelijke hiërarchie die van de formele hiërarchie afwijkt. Omdat de structuurkenmerken het gevolg zijn van de inrichting en vormgeving van de politieorganisatie, nemen wij het standpunt in dat de politie aan een ingrijpende reorganisatie toe is. Onze verwachting is dan ook dat de nationale politie met name een grote invloed op de structuurkenmerken zal hebben. Immers: het gaat om een reorganisatie van ongekende omvang en reorganisaties treffen in eerste instantie de structuur van een organisatie.

In deze subsectie zullen wij op de structuurkenmerken ingaan en formuleren we vier mogelijke oplossingen voor de problemen die voortvloeien uit de structuurkenmerken. Het gaat om (1) vermindering van de autonomie van de afzonderlijke korpsen, (2) een duidelijk landelijk beleid met betrekking tot ICT, (3) meer duidelijkheid in de taakverdeling tussen de CIE, RIO en de tactische opsporingsteams, en (4) het benutten van de informele hiërarchie van de politie bij de sturing.

Zoals gezegd moet de autonomie van de afzonderlijke korpsen drastisch worden verminderd (oplossing 1). Met de vorming van een nationale politie zal er op korpsniveau formeel een einde worden gemaakt aan de autonomie van de regiokorpsen en hiermee zal een deel van de fragmentatie worden opgelost. Met betrekking tot de ICT-problemen (zij vormen een onderdeel van het eerste structuurkenmerk) zijn wij van mening dat er op landelijk niveau een duidelijker beleid dient te komen met betrekking tot ICT voorzieningen, waarbij de uiteindelijke gebruiker centraal staat (oplossing 2). Wij sluiten ons hier uitdrukkelijk aan bij de laatste rapportage van de Algemene Rekenkamer (2011). Ook hierin zal de nationale politie beter in kunnen voorzien. Een éénduidig ICT-beleid wordt binnen de nationale politie op één, centraal niveau vastgesteld (zie Ontwerpplan Nationale Politie 2011: 34). Wij zullen hier dan ook wat langer bij de nationale politie stilstaan.

Met betrekking tot het tweede hardnekkige structuurkenmerk, de onderlinge concurrentie tussen de afdelingen, nemen wij het standpunt in dat er meer duidelijkheid moet komen omtrent de taakverdeling tussen de CIE, de RIO en de tactische opsporingsteams (oplossing 3). Met betrekking tot de CIE betekent dit specifiek dat zij de taak die zij wettelijk heeft toebedeeld gekregen ook daadwerkelijk moet gaan uitvoeren. Er moet ook een situatie worden gecreëerd waarbij de verschillende afdelingen complementair aan elkaar zijn in plaats van dat ze elkaar beconcurreren. Binnen de recherche zal er meer duidelijkheid moeten komen over de rol van de RIO's in relatie tot deze wettelijke CIE-taak. Omdat de RIO een deel van de CIE-taak uitvoert, ligt het in de lijn der verwachtingen dat zij wordt aangemerkt als CIE en ook onder het gezag van de CIE-officier valt (oplossing 3a). Op deze manier wordt er meer recht gedaan aan de situatie zoals de wetgever die oorspronkelijk voor ogen had. De RIO's opereren nu in een soort juridisch niemandsland, waarbij de rol van het hoofd CIE formeel juridisch erg groot is, maar in de praktijk is gemarginaliseerd. Hij is echter wel formeel verantwoordelijk voor de CIE. Vanuit een zuiver juridisch oogpunt is het dan ook aan te bevelen om het onderscheid tussen de CIE en de RIO op te heffen(zie ook sectie 9.7).

De hierboven genoemde oplossing (het opheffen van het onderscheid tussen de CIE en de RIO) heeft onze voorkeur. Een tweede mogelijkheid die echter meer recht doet aan de gegroeide praktijk binnen de politie is dat de analysetaak in de WPG en de overige relevante regelgeving wordt losgekoppeld van de CIE-taak en bij een RIO wordt neergelegd (oplossing 3b). De organisatorische eenheid van de CIE blijft dan belast met het verzamelen van informatie door middel van het runnen van informanten en de analisten die bij deze eenheid werkzaam zijn kunnen gericht op de ondersteuning van het runnen van informanten worden ingezet. Dit is de benadering die binnen de nationale politie is gekozen (zie Ontwerpplan Nationale Politie 2011: 41). De CIE wordt (evenals de RID) een onderdeel van de RIO. Een andere eenheid van de RIO is de afdeling Onderzoek en Analyse. In die afdeling zijn alle analisten van het district (of de landelijke eenheid) ondergebracht, dus ook de analisten die thans voor de CIE werken. Het idee lijkt te zijn dat analyse en intelligence op zichzelf staande expertises zijn: de analist beschikt over een standaard-set van basisvaardigheden en het maakt niet uit of de analist op een tactisch onderzoek naar overvallen wordt ingezet of op langlopende onderzoeken naar terrorisme of georganiseerde criminaliteit. Door een andere afdeling binnen de RIO verantwoordelijk te maken voor de analysetaak lijkt de onderlinge concurrentie vanwege eenduidige taakstelling op dit punt te zijn geslecht. De CIE kan zich toeleggen op het runnen van de informanten en voor de noodzakelijke analyses analisten van de afdeling Onderzoek en Analyse gebruiken. Overigens zal de huidige situatie waarschijnlijk voort blijven bestaan. De analisten die CIE-werkzaamheden verrichten zullen voor een langere periode bij de CIE worden gedetacheerd. Het is immers ondenkbaar dat analisten voor een paar maanden bij de CIE komen, daar in aanraking komen met zeer gevoelige informatie en vervolgens elders verder aan de slag gaan. Dit wordt door de CIE niet geaccepteerd. Feitelijk zal er voor de analisten bij de CIE dus weinig veranderen.[301] Wij merken overigens op dat dit vanuit een juridisch perspectief nog steeds een onwenselijke situatie is: de RIO vervult een groot deel van haar analysewerkzaamheden in het kader van de CIE-taak en feitelijk is zij daarmee (formeel juridisch) CIE. Het feit dat de analysefunctie organisatorisch elders is ondergebracht, doet dus niets af aan het feit dat de CIE formeel juridisch nog steeds belast is met het analyseren van de zware (georganiseerde) criminaliteit.

Het is volgens ons overigens geen goed idee om de analysecapaciteit bij de CIE weg te halen en de analisten bij een RIO te plaatsen. Om goede analyses te maken, moeten analisten dichtbij de verzameling van de informatie zitten. Dit geldt met name voor een CIE, waarbij veel informatie niet volledig in de systemen staat en waarbij analisten die niet 'volwaardig' deel uitmaken van de CIE geen toegang hebben tot de meest gevoelige informatie. Ook die informatie moet echter worden geduid, en analisten zijn hiervoor onmisbaar. En deze informatie krijgt de analist alleen maar indien er sprake is van vertrouwen tussen de analist en de runners. Zonder vertrouwen zal de analist niet over de meest actuele en juiste informatie beschikken. En vertrouwen wordt slechts gerealiseerd indien er de ruimte en mogelijkheid is voor direct onderling contact tussen de analist en de runners. Direct contact tussen de runners en de analisten is dan ook een meerwaarde voor het algemene analyseproces en de kwaliteit van de analyse. De CIE-analyse kan echter wel beter worden afgestemd op de kerntaak van de CIE: het verzamelen van informatie. De overige analysewerkzaamheden worden dan door de RIO uitgevoerd. Alhoewel deze

[301] Dit geldt niet voor de analisten die bij andere organisatieonderdelen zij ondergebracht. De kans dat zij voor verschillende klussen zullen gaan rouleren, is erg groot. Hoe dat in de praktijk zal uitwerken, zal de toekomst leren.

oplossing wellicht de voorkeur verdient omdat het recht doet aan de met de implementatie van IGP ingeslagen koers, is het nog maar de vraag of hiermee de bestaande problemen met betrekking tot informatie-uitwisseling niet worden verergerd omdat er (nog) meer afstand tussen de CIE en de RIO wordt gecreëerd. Dit zou het proces van *in-* en *outgroup*-vorming kunnen versterken. Wij zijn echter van mening dat dit niet het geval hoeft te zijn: vandaag de dag is immers ook al sprake van *in-* en *outgroup*-vorming, maar nu hebben de organisaties daadwerkelijk beide een vergelijkbare taak die onnodige concurrentie leidt. Door een duidelijke differentiatie in de taak van de CIE en de RIO aan te brengen, maar de CIE toch onder te brengen bij de RIO, zal deze concurrentie wellicht verminderen hetgeen mogelijk een remmende werking op *in-* en *outgroup*-vorming kan hebben. *In-* en *outgroup*-vorming als onderdeel van sociale categorisatie kent echter meer aspecten dan een verschil in taakstelling. Deze komen aan bod bij de discussie met betrekking tot de weerbarstige politiecultuur.

Met betrekking tot het derde structuurkenmerk zijn wij van mening dat de politie minder *top down* de veranderingen moet willen doorvoeren, en meer moet proberen om de informele hiërarchie te benutten (oplossing 4). De vrijheid van het politiewerk is één van de bijzondere aspecten van dat werk en zal gerespecteerd moeten worden wil er sprake kunnen zijn van een goede implementatie van IGP. Tegelijkertijd (en paradoxaal) is er een actievere sturing noodzakelijk waarbij consequenties worden verbonden aan het voldoen aan de informatievragen. Wij zijn van mening dat er meer sturing plaat dient te vinden op wat de runners aan informatie moeten binnenhalen en wat de analisten analyseren, maar dat hoe de medewerker dit precies doet grotendeels aan hem wordt overgelaten.

Hoe de nationale politie met dit derde structuurkenmerk omgaat, is erg interessant. In eerste opzicht zal de nationale politie naar alle waarschijnlijkheid weinig kunnen doen aan de hiërarchieproblemen. Immers, ook na de reorganisatie zal de politie een *street-level bureaucracy* zijn en heeft de medewerker op straat meer vrijheid dan de leidinggevenden. In het ontwerpplan menen wij te lezen dat de de opstellers van het plan hiervan doordrongen zijn en voornemens zijn deze ruimte te benutten in plaats van vanuit een strakke hiërarchie de werkzaamheden op straat te sturen. Wij citeren het ontwerpplan: "*Het herstel van de positie van vakmanschap en 'professionele ruimte' vraagt om een heroriëntatie op de rol van leiderschap en sturing binnen de Nederlandse politie. Het politiewerk dient centraal te staan, van het strategisch tot het operationeel niveau. Dit betekent concreet dat leiderschap en sturing ten dienste staan van de mannen en vrouwen die het werk doen: de vakmensen van de Nationale Politie*" (Ontwerpplan Nationale Politie 2011: 13). Later in het ontwerpplan wordt ook aangegeven dat het politiewerk soms vraagt om optreden buiten protocollen en regels om: niet al het politiewerk valt te regelen en vast te leggen (Ontwerpplan Nationale Politie 2011: 13). Het lijkt erop dat de opstellers van het ontwerpplan zich bewust zijn van het belang van sturing op maat. Als leidinggevenden bij de daadwerkelijke invoering van de nationale politie en tijdens de dagelijkse sturing leren om het politiewerk te beïnvloeden binnen de context van de *street-level bureaucracy*, dan zal dit mogelijk een deel van de barrières waar men in de praktijk tegenaan loopt weg kunnen nemen. Wij merken hierbij wel op dat hiervoor ook mogelijk een nieuwe lichting leidinggevenden nodig is die deze benadering durven toe te passen. Voorts is het ook nog maar de vraag in hoeverre de in het ontwerpplan verwoorde ambities haalbaar zijn: zal het negeren van de protocollen en regels inderdaad in bepaalde gevallen ongestraft blijven, of grijpen leidinggevenden terug naar de zekere weg en kiezen ze voor sancties? En in welke

gevallen sanctioneer je het niet volgen van protocollen en regels? Kortom, dit kan in de praktijk heel anders uitpakken dan in het ontwerpplan wordt geschetst. Desalniettemin geven de opstellers van het stuk blijk van realisme en kennis van de informele hiërarchie en dat is vergeleken met de situatie omtrent IGP al een hele verbetering.

D: De weerbarstige politiecultuur

De door ons geconstateerde cultuurkenmerken zijn (1) conservatieve insteek van CIE-medewerkers, (2) de waan-van-de-dag-mentaliteit, (3) de *need to know*-cultuur en (4) het proces van sociale categorisatie. Wij zullen hier voor elk van de cultuurkenmerken mogelijke oplossingen bediscussiëren. Voordat wij de kenmerken behandelen, eerst een korte opmerking over cultuurveranderingen *an sich* en de wijze waarop de nationale politie hier mee omgaat.

Een cultuur is veel lastiger te veranderen dan een structuur en daar lijken de opstellers van het ontwerpplan zich van bewust (zie Ontwerpplan Nationale Politie 2011: 14). Desalniettemin is de ambitie erg groot: er moet uiteindelijk sprake zijn van één nationale politiecultuur. We lezen in het ontwerpplan: "*Voor het behalen van het gewenste prestatieniveau van de politie is het cruciaal dat een cultuur van eenheid wordt ontwikkeld. Dit impliceert, op alle niveaus, een grondhouding waarin het lokale of regionale "eigenbelang" ondergeschikt is aan het algemeen belang, en waarin centraal staat dat de politie één en ondeelbare visie heeft op het politiewerk en de beheersmatige ondersteuning daarvan. De opdracht is om, naast de wijzigingen in structuur, ook echt één politieorganisatie te zijn, in denken en in handelen*" (Ontwerpplan Nationale Politie 2011: 12). Hoe dit het beste bereikt kan worden werd in het najaar van 2011 geïnventariseerd en aan de hand van die inventarisatie moesten er 'cultuurinterventies' worden benoemd en, na de reorganisatie zelf, dienen deze te worden uitgevoerd. Wij hebben echter geen concrete aanknopingspunten om de wijze waarop de nationale politie invloed zal hebben op de door ons benoemde cultuurkenmerken te beoordelen. Er is echter één uitzondering. Dat betreft het vierde kenmerk: de sociale categorisatie. Dit is nauw verbonden met het structuurkenmerk van concurrentie en wij zullen dan ook stilstaan bij de wijze waarop de nationale politie de sociale categorisatie beïnvloedt. Bij de discussie omtrent de sociale categorisatie zullen wij stilstaan bij de nationale politie.

Voor alle door ons geconstateerde cultuurproblemen geldt dat ze slechts kunnen worden opgelost indien er sprake is van (A) een mentaliteitsverandering bij de bestaande medewerkers, of dat er (B) actief wordt geprobeerd de samenstelling van de CIE te vernieuwen. Wij zijn van mening dat met name de laatste optie kan leiden tot een verandering in de CIE-cultuur, waardoor IGP succesvol geïmplementeerd kan worden. Er moeten meer medewerkers worden aangetrokken die niet wars zijn van innovaties en veranderingen en die daarnaast niet zijn gevormd door een reactieve politiepraktijk. Deze medewerkers moeten beter in staat zijn om zich (1) los te maken van het traditionele, reactieve politiewerk en (2) meer proactief en op lange termijn te denken. Wij zijn ons overigens bewust van de angst binnen de CIE dat hierin wordt doorgeschoten. De traditionele CIE-ers blijven volgens ons zeker ook nodig, omdat een aanzienlijk deel van het CIE-werk nooit zal veranderen: er zal bijvoorbeeld altijd een ondersteunende rol voor de CIE zijn weggelegd bij de tactische opsporingsonderzoeken. Daarnaast beschikt een aantal oudere medewerkers over bijzonder veel kennis en ervaring die niet terug te vinden is in de informatiesystemen. Deze kennis en kunde moeten ten volste benut worden. Wij zijn daarom van mening

dat een systeem waarbij een ervaren CIE-er een aantal van de nieuwe collega's onder zijn hoede neemt en begeleidt, kan leiden tot het beste van beide werelden: zowel de ervaring en kennis van de oudere medewerker, als de proactieve en lange-termijn-benadering van de nieuwe medewerkers. Dit brengt overigens weer zijn eigen problemen met zich mee (dat geldt voor alle mogelijke oplossingen voor de door ons geconstateerde problemen). Wij menen echter wel dat een belangrijk deel van de nieuwe CIE-medewerkers een afwijkend profiel dient te hebben van de traditionele CIE-runners, waarbij in ieder geval kan worden gedacht aan een bepaalde opleidingsachtergrond of ervaring in een andere sector dan de politie. Een andere optie is de bestaande CIE-medewerkers een opleiding aan te bieden waarin oog is voor proactief werk en lange-termijn-denken.

In eerste instantie zal het aantrekken van nieuwe collega's van buiten de politieorganisatie leiden tot verzet bij de bestaande medewerkers. Daarom is het van groot belang dat de nieuwe instroom een aanzienlijk aantal medewerkers betreft die binnen dezelfde teams werken: indien de groep te klein is, zullen de nieuwe medewerkers kwetsbaar zijn en niet worden opgenomen en geaccepteerd binnen de groep, of ze worden door de bestaande organisatie geassimileerd. In het geval van assimilatie wordt de doelstelling van cultuurverandering niet behaald. Het gaat hier echter te ver om deze (potentiële) nieuwe problemen uitgebreid te behandelen. Hiervoor is meer onderzoek nodig.

Met betrekking tot de *need to know*-cultuur (cultuurkenmerk 3) stellen wij ons op het standpunt dat men eerst de oorzaken van de geheimhouding dient vast te stellen voordat er oplossingen worden aangedragen en geïmplementeerd. Met andere woorden, voordat er een *need to share* beweging wordt ingezet, zal moeten worden onderzocht wat nu precies het probleem is en hoe groot dat probleem is. Wij hebben meerdere redenen voor geheimhouding benoemd, maar wij waren niet in de positie of gelegenheid om te onderzoeken welke redenen in welke mate een rol spelen. Hiervoor is een verdergaand onderzoek naar de informatie van de CIE nodig. Ironie wil overigens dat een onderzoek naar de redenen voor geheimhouding *omwille van redenen van geheimhouding* bijna alleen intern door de CIE kan worden uitgevoerd. Het zou echter het beste zijn om een externe persoon of instantie een dergelijk onderzoek uit te laten voeren, dit om te voorkomen dat de slager zijn eigen vlees keurt.

Wanneer de oorzaken voor geheimhouding zijn vastgesteld, moet er gericht worden geprobeerd om deze oorzaken weg te nemen indien ze niet operationeel van aard zijn. Institutionele redenen van geheimhouding kunnen bijvoorbeeld worden weggenomen indien het delen van informatie mogelijk is zonder dat dit ten koste gaat van invloed en autonomie. Daarnaast zou de kosten/baten afweging in het voordeel van de baten van het delen van informatie moeten doorslaan: de medewerker moet worden gestimuleerd om daadwerkelijk informatie te delen. Dit betreft de derde institutionele reden van geheimhouding (zie sectie 9.1). Er moet iets tastbaars staan tegenover het delen van informatie die de kosten/baten inschatting doet doorslaan naar de baten. Dit kan bijvoorbeeld door het delen van informatie een onderdeel te maken van het functioneringsgesprek van de medewerker. Het delen van informatie leidt tot een goede beoordeling, en het onterecht niet delen van informatie leidt tot een slechte beoordeling.

Deels kan het behoud van invloed en autonomie worden bereikt met de oprichting van één landelijke CIE waar het gaat om de verzameling van informanteninformatie. Er kan dan een eenduidige lijn worden gekozen met betrekking tot het delen van informatie, hetgeen in ieder geval voorkomt dat CIE-en

onderling geen informatie uitwisselen omdat andere CIE-en teveel informatie delen met bijvoorbeeld een RIO. Wij zijn ons er verder wel van bewust dat het oprichten van een landelijke afdeling CIE op veel organisatorische en budgettaire bezwaren zal stuiten. Het gaat in het kader van ons onderzoek echter te ver om hier dieper op in te gaan: hiervoor is extra onderzoek nodig.

Een oplossing voor de problemen die voortvloeien uit de sociale categorisatie (cultuurkenmerk 4) is dat er een einde wordt gemaakt aan de onderlinge concurrentie tussen de CIE en de andere onderdelen van de opsporing, te weten de tactische onderzoeksteams en de RIO (dit hebben wij al behandeld bij de structuurkenmerken). Wij zijn ons er echter van bewust dat een zekere mate van sociale categorisatie en concurrentie niet te voorkomen is. Dit zal altijd een onderdeel uitmaken van grote bureaucratische organisaties. Zelfs als de CIE en de RIO worden samengevoegd, zal er een bepaalde mate van concurrentie plaatsvinden. De processen die ten grondslag liggen aan sociale categorisatie zijn nu eenmaal complex en zullen niet worden opgelost door de organisatorische knip tussen de inwin- en analysefunctie. Er is immers één element waarover altijd concurrentie zal blijven bestaan: de informatie van de CIE. Immers, het feit dat de CIE wordt opgenomen in de RIO betekent niet dat de andere onderdelen van de RIO automatisch toegang krijgen tot de CIE-gegevens. Met de autorisaties voor deze bijzondere categorie van politiegegevens zal nog steeds erg voorzichtig moeten worden omgegaan. Zoals we hebben betoogd, is er in de perceptie van andere partijen vrijwel automatisch spraken van een ongerechtvaardigde geheimhouding. Vanuit het perspectief van de CIE zullen zij actief de gegevens moeten afschermen, en dit leidt wellicht tot een versterkte sociale categorisatie.

Alhoewel de CIE organisatorisch bij de RIO wordt ondergebracht, is het dan ook nog maar de vraag of dit zal leiden tot de binnen de nationale politie gewenste cultuur van (nationale) eenheid. Sterker nog, een aantal CIE-en die vandaag de dag nog niet zijn ondergebracht bij de RIO zien deze beweging met grote bedenkingen tegemoet. Zij zijn bang dat de RIO uiteindelijk toegang tot de informatie van de CIE zal wensen, en deze CIE-ers vrezen dan ook voor de bronafscherming. En ondanks de nieuwe organisatorische inbedding, blijft de CIE een organisatieonderdeel dat zich grotendeels afschermt van de buitenwereld. Die ruimte en mogelijkheid heeft zij ook. Daarnaast doet de voorgenomen reorganisatie niets aan de wijzen waarop de CIE-ers 'verzet' kunnen plegen tegen de door hen gevreesde ontwikkelingen (de 'terugkeer naar het zakboekje'). De inlijving van de CIE bij de RIO kan zelfs een extra stevige reactie opleveren. In dit scenario hebben de CIE-ers het gevoel ondergeschikt te worden gemaakt aan andere organisatieonderdelen (in casu de RIO), hetgeen een verregaande *ingroup*-vorming zal veroorzaken. Dat ze onderdeel worden van de RIO bevestigt voor deze medewerkers hun ondergeschikte rol, met als mogelijk effect dat zij zich nog sterker een *ingroup* voelen die zich moet verweren tegen de buitenwereld (lees: de informatie dient af te schermen). Of en in hoeverre dit daadwerkelijk gebeurt, kunnen wij op voorhand natuurlijk niet inschatten. Gezien de bevindingen van ons onderzoek is het echter geen denkbeeldig scenario.

Wat wij op voorhand ook een reëel risico achten, is de verregaande verzuiling en toenemende scheiding tussen de analysefunctie en de recherchefunctie (de CIE daarbij inbegrepen). Wij constateren dat binnen de (nationale) politie het idee leeft dat intelligence en informatie op zichzelf zijnde disciplines zijn die los staan van de overige operationele werkzaamheden van de politie. Dit wordt nog eens bevestigd door het feit dat alle analisten bij een aparte afdeling van de RIO worden ondergebracht. De CIE heeft dan formeel geen analisten meer, maar krijgt analisten van de afdeling Onderzoek en Analyse. Maar ook hier wordt in het ontwerpplan

rekening mee gehouden. Er valt namelijk te lezen dat opsporing en intelligence met elkaar verbonden moeten zijn (Ontwerpplan Nationale Politie 2011: 29). We citeren uit het ontwerpplan: "*De DRIO is lokaal verbonden en verankerd. Medewerkers van de DRIO zijn gedeconcentreerd fysiek aanwezig binnen de onderdelen van de eenheid*" (Ontwerpplan Nationale Politie 2011: 41). Hiermee lijkt de kloof tussen de operationele activiteiten en analyse juist te worden verkleind. Wij wijzen echter op het gegeven dat het er helemaal van afhangt of de analisten voor een langere termijn op afdelingen en/of onderzoeken worden geplaatst, of dat het kortlopende trajecten zijn. Voor het vertrouwen tussen analisten en andere politiemedewerkers is het van belang dat dezelfde analist gedurende langere tijd op één afdeling aan één onderwerp werkt. Indien voor iedere opdracht een andere analist wordt gekozen, zal er van vertrouwen en een daadwerkelijke vervlechting van intelligence en operationele activiteiten geen sprake zijn. Voorts zijn wij van mening dat het voorgaande ook geldt voor de strategische analisten. Zij dienen ook dicht bij de operationele werkzaamheden te zitten, zodat ze optimaal invulling geven aan wat wij eerder 'strategisch denken in intelligence' hebben genoemd. Hoe met deze vraagstukken zal worden omgegaan, kan nu echter nog niet worden gezegd. Hiervoor dienen de plannen eerst verder uitgewerkt te worden.

De door ons voorgestelde veranderingen zijn zeer ingrijpend en diepgaand. Ze kosten tijd, geld en zijn risicovol, drie elementen die doorgaans ontwikkelingen binnen de overheid in het algemeen en de politie in het bijzonder tegenhouden. Echter, om IGP om te vormen van een concept naar de praktijk zijn deze aanpassingen wel noodzakelijk. Ze verdienen het in ieder geval om binnen de politie te worden bediscussieerd. We signaleren dan ook met voorzichtig optimisme dat de nationale politie in ieder geval op papier een goede eerste stap in de richting van de noodzakelijke veranderingen zet. Wij zijn echter *voorzichtig* optimistisch omdat we onder andere uit ons eigen onderzoek weten dat de papieren werkelijkheid vaak afwijkt van de praktijk.

9.6.2 De verhouding tussen de AIVD en de CIE

Met betrekking tot de verhouding tussen de AIVD en de CIE hebben wij vastgesteld dat er conceptueel belangrijke verschuivingen plaatsvinden die meer interactie tussen de AIVD en de CIE als gevolg zullen hebben. Alhoewel deze ontwikkelingen in de praktijk (veel) minder snel gaan dan in theorie, willen wij er toch nog bij stil staan. Ook zullen wij kort de invloed van de nationale politie op de ontwikkelingen behandelen. Wij behandelen allereerst (A) de vraag naar de normatieve bezwaren van een veranderende verhouding. Vervolgens (B) geven wij mogelijke oplossingen die meer interactie tussen de organisaties mogelijk zal maken.

A: Normatieve bezwaren

Omdat de scheiding tussen veiligheidsdiensten en de politie kan worden gezien als één van de kenmerken van een democratische rechtsstaat, zullen veranderingen die invloed op die scheiding hebben leiden tot discussies. In hoofdstuk één hebben we de belangrijkste argumenten tegen de vermenging van de veiligheidsdiensten en de politie al genoemd (zie sectie 1.7). Wij zullen ze hier kort herhalen. Het eerste argument is dat de scheiding tussen de veiligheidsdiensten en de politie een waarborg vormt voor de adequate bescherming van persoonsgegevens. Een vermenging van deze diensten zal aldus leiden tot een verminderde bescherming van

persoonsgegevens. Het tweede argument is dat de scheiding voorkomt dat informatie te snel uit een bepaalde context wordt gehaald en verkeerd wordt begrepen. Wanneer beide diensten vermengen, bestaat het gevaar dat informatie verkeerd wordt beoordeeld en dat dit leidt tot verkeerde beslissingen. Het derde argument is dat de scheiding een kenmerk is van een democratische rechtsstaat en de vermenging van de diensten is het spiegelbeeld, te weten een kenmerk van een politiestaat. Een vermenging van de diensten is in dit opzicht een aanwijzing dat er mogelijk sprake is van een politiestaat. Alhoewel wij constateren dat de vermeende theoretische vermenging van de diensten in de praktijk uitblijft, willen wij wel kort stilstaan bij de genoemde bezwaren. Hierbij merken wij op dat het behandelen van deze bezwaren eigenlijk buiten het bereik van ons onderzoek valt.

Met betrekking tot het eerste argument (de vermenging leidt tot een verminderde adequate bescherming van persoonsgegevens), stellen wij vast dat hier sprake is van een reëel risico. De scheiding komt er in deze situatie op neer dat de informatiestromen van de AIVD en de politie van elkaar gescheiden dienen te blijven. Het gevaar bestaat bijvoorbeeld dat gegevens over burgers bij verschillende overheidsorganisaties terechtkomt, in casu zowel de AIVD als de politie, en dat deze gegevens daardoor moeilijk te verwijderen zijn. Voor de burger is het onmogelijk om na te gaan waar 'zijn' persoonsgegevens liggen opgeslagen. Het is voor hem onmogelijk om de gegevens verwijderd of aangevuld te krijgen indien ze onjuist, onvolledig of verouderd zijn. Dit is een reëel risico, waarbij echter moet worden aangetekend dat het nog maar de vraag is of het vasthouden aan de scheiding tussen de organisaties de belangrijkste waarborg zal zijn. Is de vermenging van de diensten hier het werkelijke probleem, of is de wijze waarop de diensten omgaan met dataprotectie-regelgeving het probleem?[302] In het verlengde hiervan merken wij op dat het *matchen* van de politiële databases tegen die van de veiligheidsdiensten *in theorie* ook een schonende werking kan hebben. De organisaties kunnen elkaars databases aanvullen, verbeteren en wellicht schonen. Uit de politiële informatie kan bijvoorbeeld blijken dat een door de AIVD waargenomen potentiële dreiging in feite geen dreiging is. Andersom kan uit AIVD-informatie blijken dat een verdenking van de politie in feite onterecht is. De relevante informatie dient in die gevallen bijvoorbeeld aangevuld, verbeterd of verwijderd te worden. Indien dit niet het geval is en de informatie blijft foutief in de systemen opgeslagen, dan is er sprake van een gebrekkig zelfreinigend vermogen van de diensten als het op de eigen databases aankomt en van het niet-naleven van dataprotectie-regelgeving. Dit is echter geen gevolg van een mindere scheiding tussen de veiligheidsdiensten en de politie. In deze situatie is het overigens wel verstandig om vast te houden aan de scheiding, omdat dit voorkomt dat het probleem nog groter wordt met het groter worden van de databases. Voorts is het de vraag of dit dataprotectie-argument opweegt tegen wat wij het 'veiligheidsargument' noemen, namelijk dat het delen van informatie leidt tot het voorkomen van bijvoorbeeld terroristische aanslagen. Deze discussie valt echter buiten het bestek van ons onderzoek.

Het tweede argument (de vermenging leidt tot het gevaar dat de context van de informatie verloren gaat), is volgens ons geen argument tegen de vermenging van de diensten, maar juist een argument voor een verdergaande vermenging. Immers, als het probleem is dat de context verloren gaat betekent dit niet automatisch dat de diensten dan maar gescheiden moeten opereren. Integendeel: er moet meer interactie zijn

[302] Hiermee zeggen wij overigens niet dat er een probleem is op het gebied van naleving van deze elementen van dataprotectie-regelgeving . Dit valt echter niet binnen het bereik van ons onderzoek en hier zullen we daarom niet verder op ingaan.

tussen de AIVD en de politie in de zin van afstemming en operationele samenwerking zodat dit context-probleem kan worden voorkomen. Dit zorgt er immers voor dat de contextuele factoren kunnen worden meegenomen in de waardering van de informatie en pleit dus eigenlijk voor een verdergaande vermenging van de diensten dan thans het geval is. Een afgeleide van dit argument is dat de AIVD bij uitstek in staat is om met 'zachte informatie' te werken, en dat de politie de benodigde kennis en expertise niet zou hebben (zie CBP 2004; zie ook sectie 1.7).[303] Wij zijn het hier niet mee eens. De AIVD-informatie is niet per definitie zacht omdat het van de AIVD is. Het kan ook 'harde informatie' zijn, bijvoorbeeld afkomstig uit telecomgegevens of telefoontaps. Politie-informatie afkomstig uit vergelijkbare bronnen wordt aangemerkt als harde informatie en kan in dit opzicht worden gebruikt als bewijs. Het verschil is dat de AIVD sneller bepaalde bevoegdheden kan inzetten dan de politie. Dit zegt echter niets over het 'harde' of 'zachte' gehalte van de informatie. Voorts is de veronderstelde expertise die nodig is om met deze informatie te werken al jaren bij de politie aanwezig. Ook de politie werkt met informatie uit telefoontaps en vergelijkbare soorten informatie. En daar waar specifieke inhoudelijke kennis nodig is van bepaalde fenomenen zoals terrorisme, is de politie hard op weg om zelf expertise binnen de organisatie te krijgen. Dit kan overigens ook een argument zijn om de expertise onderling uit te wisselen (iets dat overigens op ander hoog-specialistische terreinen al lang gebruikelijk is, zoals het heimelijk plaatsen van afluisterapparatuur). Al met al is dit tweede argument volgens ons niet echt sterk. We zijn aangekomen bij het derde argument tegen de vermenging.

Het derde, rechtsstatelijke argument is in een zeker opzicht het minst objectieve en minst concrete argument. Het raakt aan bepaalde normen, waarden en de daarbij behorende politieke (en sociaal-maatschappelijke) overtuigingen. Dit argument is dan ook erg moeilijk om objectief te beoordelen. Wij zullen hier toch een poging doen.

Onzes inziens is een vermenging van de veiligheidsdiensten en de politie op zichzelf niet direct een kenmerk van een politiestaat. Het is immers niet de scheiding tussen de diensten die een staat tot een politiestaat maakt. Een politiestaat is meer dan dat. In het enige ons bekende boek over de politiestaat *an sich* wordt de volgende definitie gegeven: "*a political unit (as a nation) characterised by repressive governmental control of political, economic and social life usually by an arbitrary exercise of power by the police, and especially the secret police, in place of the regular operation of the administrative and judicial organs of government according to established legal processes*" (Chapman 1970: 53). Om van een politiestaat te kunnen spreken dient het optreden van de (geheime) politie dus arbitrair, ongecontroleerd en niet-transparant te zijn. Voorts moet er sprake zijn van een repressieve overheidscontrole van het politieke, economische en sociale leven. De voorbeelden van dergelijke politiestaten zijn nazi-Duitsland, de Sovjet-Unie en Noord-Korea. Het gaat ons te ver om in de Nederlandse situatie te spreken van een politiestaat: de AIVD en de politie vertonen weliswaar steeds meer onderlinge gelijkenis, maar dit maakt ze nog geen Gestapo of KGB. Dit komt met name omdat de politieke context van Nederland een democratische rechtsstaat is: er is geen totalitair regime aan de macht, de overheid dient zich ook aan wetgeving te houden en de veiligheidsdiensten en politie zijn niet belast met het aan de macht houden van een dergelijk regime. Daarnaast is er onafhankelijke rechtspraak en zijn de AIVD en de

[303] Het CBP stelt dit in een advies omtrent het (destijds) concept-wetsvoorstel inzake de bijzondere bevoegdheden tot opsporing van terroristische misdriiven, meer specifiek het gebruik van het criterium van de voorwaarschuwing in plaats van de verdenking. Zie ook subsectie 4.4.4.

politie gebonden aan wet- en regelgeving. De verschillen met de bekende voorbeelden van politiestaten zijn dan ook erg groot. Wij zijn van mening dat het de politieke context is die uiteindelijk maakt of er gesproken kan worden van een politiestaat. De scheiding tussen veiligheidsdiensten en de politie biedt echter wel een waarborg tegen een ongecontroleerde, geheime politieke politie. Wij vergelijken het uiteindelijke gevaar van een te grote (conceptuele) vermenging van veiligheidsdiensten en de politie met het dragen van autogordels. Een bestuurder die geen autogordel draagt, raakt niet daarom direct betrokken bij een ongeval. Maar als hij onverhoopt toch bij een ongeval betrokken raakt, dan zijn de gevolgen vaak vele malen groter. En autogordels zijn niet de enige veiligheidsmaatregelen waar in het verkeer gebruik van wordt gemaakt. Hetzelfde geldt voor de veranderende verhouding tussen veiligheidsdiensten en opsporingsdiensten. Indien de scheiding tussen deze diensten wegvalt, betekent dit nog niet dat er automatisch grote gevolgen voor de rechtsstaat zijn. Maar als het fout gaat, zijn de gevolgen veel groter. Dit maakt dat er waarborgen moeten worden ingebouwd die de nadelige gevolgen van een vermenging tegengaan. Met andere woorden: de nadelige gevolgen dienen te worden gecompenseerd. Het gaat te ver om hier alle mogelijke waarborgen te behandelen. Wij zullen kort stilstaan bij wat volgens ons de belangrijkste waarborg kan vormen: de toetsing op de rechtmatigheid van het optreden in de informationele voorfase ('intelligence-fase' in het jargon).

Wanneer het optreden van de diensten een inbreuk maakt op fundamentele rechten, dient er sprake te zijn van voldoende controle en transparantie van de diensten. In de huidige situatie is er sprake van een redelijk verregaande toetsing en controle: voor de AIVD is de Commissie van Toezicht hiermee belast, en voor de politie zijn het OM, de rechter en het CBP belast met de controle op de opsporing en de informationele voorfase. Wij zijn echter van mening dat de door ons geschetste ontwikkelingen op het gebied van IGP en de (theoretische) vermenging van de AIVD en de CIE een risico aan de kant van de politie met zich meebrengen. De politie maakt in toenemende mate gebruik van alternatieve interventies, zoals de verstoring van mensen die in verband worden gebracht met terrorisme, en in die gevallen komt er geen strafrechter aan te pas.[304] Daarnaast wordt de informatiepositie van de politie steeds belangrijker, en in de informationele voorfase worden de werkzaamheden van de politie onvoldoende gereguleerd. Kielman (2010: 62-63) spreekt in dit kader van een 'instrumentele benadering' van de WPG en het ontstaan van informationele opsporingsmethoden die eigenlijk strafvorderlijke kenmerken in zich dragen. Een voorbeeld is *datamining*. Het toezicht en de controle op deze informationele opsporingsmethoden is thans gefragmenteerd en versnipperd en dient te worden herzien (zie ook: Kielman 2010: 218). Een politie die nauwelijks wordt getoetst en gecontroleerd, voldoet niet aan de rechtsstatelijke eis van transparantie, en hiervoor moet zeker worden gewaakt. Een mogelijke oplossing voor deze situatie is de aanstelling van een rechter-commissaris voor de informationele voorfase (de intelligence/CIE-fase) die de rechtmatigheid van de werkzaamheden van het politieoptreden toetst. Deze rechter-commissaris dient volledige inzage te hebben in al het politieoptreden in de voorfase, inclusief het runnen van de informanten en de samenwerking met de AIVD. Het vergroten van de capaciteit van het CBP is ook een optie. Op dit moment is de capaciteit van het CBP te klein om al het politie-optreden te controleren, zeker daar waar het de informationele voorfase betreft. Al met al

[304] Overigens staat bij dergelijke politie-interventies wel de weg naar de burgerlijke- of bestuursrechter open. Het gaat in het kader van dit onderzoek echter te ver om de controle door deze rechters te vergelijken met die door de strafrechter. Wij laten dit dan ook verder buiten beschouwing.

moeten er waarborgen worden ingebouwd om ervoor te zorgen dat de noodzakelijke transparantie wordt bereikt, maar wel met in achtname van de noodzakelijke afscherming. Dat dit een zeer complexe uitdaging is, mag duidelijk zijn. Desalniettemin is het een noodzakelijke voorwaarde om de potentiële vermenging in overeenstemming te brengen met de eisen die gelden binnen een democratische rechtsstaat.

Wij merken tot slot op dat het vreemd is om vast te houden aan de fictie van een scheiding tussen de veiligheidsdienst en de politie als kenmerk van de rechtsstaat wanneer geconcludeerd kan worden dat beide organisaties in theorie in toenemende mate gelijkenissen vertonen. Het zou beter zijn om de (theoretische) vermenging te accepteren en de discussie te richten op de noodzakelijke rechtsstatelijke waarborgen in plaats op het vast willen houden aan iets wat in toenemende mate tot het verleden behoort.

B: De verhouding

Dat de veiligheidsdiensten in het algemeen en de AIVD en de CIE in het bijzonder meer activiteiten moeten afstemmen, informatie moeten uitwisselen en meer moeten samenwerken zal niet snel tot discussies leiden. Een effectieve en efficiënte terrorismebestrijding vereist immers dat de betrokken organisaties elkaar niet in de weg zitten en in de wielen rijden. Hoe dit in de praktijk vorm moet krijgen, is echter de vraag.

Wij zijn allereerst van mening dat er een duidelijker onderscheid tussen de verantwoordelijkheden van de AIVD en de politie op het gebied van terrorismebestrijding dient te worden aangebracht. Immers, als iedereen verantwoordelijk wordt gesteld, is uiteindelijk niemand verantwoordelijk. De wetgever lijkt er nu voor te hebben gekozen om zowel de AIVD als de politie als taak te geven terroristische aanslagen te voorkomen, zonder dat een duidelijk onderscheid wordt gemaakt tussen de specifieke verantwoordelijkheid van respectievelijk de AIVD en de politie. Alhoewel het begrijpelijk is dat aanslagen voorkomen dienen te worden, is het vanuit een oogpunt van interactie tussen de organisaties niet verstandig om beide hiervoor verantwoordelijk te maken. Omdat het nog steeds gescheiden organisaties zijn, is de kans op concurrentie groter wanneer ze vergelijkbare verantwoordelijkheden en doelstellingen hebben. Wij zijn van mening dat de toegevoegde waarde van de politie ligt in de traditionele opsporing. De AIVD is immers verboden om aan opsporing te doen, dus hier kan de politie een bijdrage leveren. Overigens lijkt terrorisme bijzonder effectief te kunnen worden bestreden door middel van opsporing, omdat terroristen in veel gevallen niet over de vaardigheden beschikken die nodig zijn voor het succesvol plegen van criminaliteit, terwijl zij wel zijn aangewezen op criminaliteit voor bijvoorbeeld het verkrijgen van wapens en geld. Met andere woorden: een terrorist is niet zelden een slechte crimineel (Hamm 2007).

Het voorkomen van terroristische aanslagen zal volgens ons specifiek bij de AIVD moeten worden belegd, en de politie zal specifiek als taak moeten hebben terroristische misdrijven op te sporen met als doel de materiële, strafprocesrechtelijke waarheidsvinding. De neiging van de wetgever om iedereen verantwoordelijk te maken voor het voorkomen van terrorisme zonder duidelijke taakaccenten te geven, heeft ertoe geleid dat in de praktijk onduidelijk is wie nu waarvoor verantwoordelijk is. Het grote voordeel van duidelijke verantwoordelijkheden is ook dat het tegemoet komt aan de institutionele redenen voor geheimhouding. Duidelijke

verantwoordelijkheid zorgt immers voor meer behoud van invloed en autonomie, hetgeen twee van de drie institutionele redenen voor geheimhouding zijn.

Wij zijn de mening toegedaan dat de huidige praktijk van het AOT en het IOT voorziet in de behoefte om activiteiten af te stemmen. Deze overleggen zijn succesvol. Het probleem zit met name bij de stelselmatige informatie-uitwisseling en de onderlinge samenwerking.

Wij zien de geheimhouding door de AIVD als één van de grootste barrières tegen een goede stelselmatige informatie-uitwisseling en samenwerking. Met betrekking tot informatie-uitwisseling stellen wij ons dan ook op het standpunt dat met name de AIVD meer informatie aan de politie zou moeten verstrekken. De samenwerking zal meer op basis van gelijkwaardigheid moeten plaatsvinden, en dit kan alleen wanneer beide organisatie naar elkaar open zijn. Een CT-infobox is hiertoe een goede eerste aanzet, maar wij merken hierbij op dat duidelijker moet worden dat de CT-infobox een samenwerkingsverband is en dat de partijen op basis van gelijkwaardigheid informatie uitwisselen en gezamenlijk terrorismegerelateerde subjecten en onderwerpen analyseren. De grote rol van de AIVD zal hierbij kleiner gemaakt moeten worden. Het is onzes inziens wenselijker om een organisatie als de CT-infobox bijvoorbeeld bij de NCTb onder te brengen. Dit is immers de instantie die is belast met een overkoepelende coördinerende rol als het gaat om terrorismebestrijding en het is daarmee niet meer dan logisch dat deze organisatie een samenwerkingsverband als de CT-infobox faciliteert en aanstuurt. Wij zijn ons ervan bewust dat het door ons voorgestelde tegen juridische, organisatorische en culturele bezwaren stuit, met name bij de AIVD. Deels kan dit worden ondervangen door bijvoorbeeld de mogelijkheden voor verstrekking door de AIVD aan de politie/CIE in de WIV te verruimen. Wij merken hierbij op dat bij een onderwerp als terrorisme juridische en organisatorische bezwaren zelden daadwerkelijke belemmeringen zijn gebleken. Wetten kunnen worden gewijzigd en reorganisaties worden ingezet en doorgevoerd. Dat het hier gaat om een gevoelig onderwerp als terrorismebestrijding en de AIVD noopt tot de noodzaak van adequate voorzieningen met betrekking tot bijvoorbeeld geheimhouding, maar dit moet allemaal te organiseren zijn. Het werd immers bij de oprichting van de CT-infobox ook van de politie en de andere organisaties verwacht dat zij fysiek naar de AIVD zouden komen en onder aansturing en verantwoordelijkheid van deze dienst zouden vallen, juridische, organisatorische en culturele bezwaren ten spijt. Dit zal dan ook mogelijk moeten zijn bij de AIVD. De NCTb zal zich meer dan nu het geval is moeten richten op de ondersteuning van de operationele organisaties (zoals de AIVD en de politie).

Wij menen dat de grootste uitdaging ligt in het opbouwen van een vertrouwensrelatie en het wegnemen van bepaalde barrières tegen het delen van informatie. De vraag is dan ook of een organisatorische oplossing zoals beoogd met een CT-infobox of een juridische oplossing zoals het wijzigen van de WIV daadwerkelijk een oplossing zal zijn voor het probleem van de gebrekkige samenwerking en het ontbreken van vertrouwen. Het draagt bij aan een meer gelijkwaardige relatie tussen de onderlinge partijen, maar dat is slechts één ingrediënt van vertrouwen. We moeten oppassen voor het aandragen van nieuwe bureaucratieën alsof die een oplossing zijn voor het probleem van de bureaucratie. Juridische en organisatorische ordeningsprincipes winnen het als vermeende oplossing vaak van sociale ordeningsprincipes, terwijl juist in die sociale ordeningsprincipes de oorzaak van veel problemen ligt. Het risico is immers dat er nog een bureaucratische organisatie wordt opgetuigd die door geen van de partijen wordt vertrouwd en de zoveelste concurrent op het gebied van de terrorismebestrijding vormt.

Wij stellen ons daarom op het standpunt dat de daadwerkelijke oplossing voor het vertrouwensprobleem veel meer gezocht moet worden in sociale ordeningsmechanismen, zoals een netwerkbenadering in plaats van een bureaucratische organisatie. Net zoals wij hierboven hebben beschreven voor de implementatie van IGP, zal er met name moeten worden geïnvesteerd in structuur- en met name cultuurveranderingen. Vertrouwen kan niet worden afgedwongen met wetgeving en reorganisaties, maar moet worden opgebouwd met oog voor de drie essentiële elementen: een min of meer gelijkwaardige positie van de betrokken partijen, een reden voor samenwerking en met name het wegnemen van het element van risico. Dat laatste kan bijna alleen worden gedaan door de negatieve perceptie van geheimhouding te bestrijden. Wij pleiten daarom voor het gebruiken van een informele informatie-infrastructuur: een variant van de *old boys networks*. Dit zal echter vanwege de operationele redenen van geheimhouding binnen de kleine wereld van de CIE en de AIVD moeten worden 'georganiseerd'. Een nieuwe bureaucratische structuur of nieuwe juridische mogelijkheden voor informatie-uitwisseling zullen onzes inziens namelijk niet leiden tot een oplossing voor de cruciale problemen die wij signaleren. Vertrouwen kan nu eenmaal niet worden gegoten in structuren of een juridisch raamwerk, maar zal langzaam moeten groeien door middel van een toenemende onderlinge interactie. Wij kunnen de meerwaarde hiervan niet beter verwoorden dan één van onze respondenten deed: "*Ik was met een jongen op pad, een AIVD-er, enne, die zei 'het zou zo mijn maat kunnen zijn'. Dat was wel leuk. En dat was ook zo met die jongen, dat was een goeie jongen*" (interview teamleider CIE (D), november 2009). Door kleine, min of meer informele netwerken te stimuleren krijgt vertrouwen meer de kans en zal uiteindelijk de informatie-uitwisseling gemakkelijker gaan. Dit zal wel stuiten op andersoortige bezwaren, bijvoorbeeld vanuit het oogpunt van rechtsbescherming (databescherming en privacy). Er zal dan ook voorkomen moeten worden dat er bijvoorbeeld U-bocht constructies ontstaan of netwerken die zich onttrekken aan iedere vorm van toetsing en controle.[305] Wij zijn van mening dat de bovengenoemde informele netwerken vanuit het perspectief van vertrouwen een goede oplossing zullen zijn, maar wij zijn ons er ook van bewust dat het nog maar de vraag is of dit voordeel opweegt tegen de nadelen. Dit zou wat ons betreft nader onderzocht moeten worden.

We zijn nu aangekomen bij de vraag op welke wijze de nationale politie de verhouding zal beïnvloeden. De eventuele invloed van de nationale politie op de verhouding tussen de AIVD en de CIE/RIO zal met name een neveneffect zijn van de reorganisatie. De reorganisatie heeft een andere doelstelling en lijkt veel directer in verband te staan met het andere onderwerp van ons onderzoek: de implementatie van IGP. Toch zijn er aspecten van de nog te vormen nationale politie die invloed kunnen hebben op de verhouding. Wij noemen de belangrijkste twee: (1) terrorismebestrijding als exclusieve taak van de landelijke eenheid en (2) de splitsing van de RID in een WIV-team en een openbare orde-team.

In het ontwerpplan van de nationale politie valt te lezen dat terrorismebestrijding exclusief belegd zal worden bij de nationale eenheid (Ontwerpplan 2011: 30; 43). Dit betekent dat er voor de districten geen taak meer is

[305] Een U-bocht constructie ziet op de situatie waarbij politiemensen informatie die zij niet mogen verwerken, bijvoorbeeld omdat deze onrechtmatig is verkregen of omdat de bewaringstermijn is verstreken, aan de AIVD geven met als doel deze van de AIVD terugverstrekt te krijgen. Daarmee wordt de verdere verwerking door de politie weer rechtmatig. Deze manier van het witwassen van informatie raakt de integriteit van de informatieverwerking door de politie en de AIVD en moet zoveel mogelijk voorkomen dienen te worden.

op het gebied van terrorismebestrijding. Dit maakt de afstemming tussen de AIVD en de politie makkelijker: er is slechts één afdeling van de politie die bij de afstemming betrokken hoeft te worden. In de huidige situatie (dus voor de nationale politie) is deze afstemming behoorlijk complex. Met name de grote korpsen zoals Amsterdam-Amstelland hebben hun eigen afdeling die zich bezighoudt met de regionale terrorismebestrijding. Die afdelingen monitoren bepaalde onderwerpen en voeren onderzoeken uit. Het operationele risico voor de AIVD van deze regionale antiterrorisme teams is aanzienlijk: op basis van hun activiteiten kunnen onderzoeken worden opgestart en uitgevoerd waar de AIVD een inlichtingenbelang in heeft. De AIVD zal veel inspanning moet leveren om, onder andere via de RID-en, zicht te krijgen op alles wat op het gebied van terrorismebestrijding plaatsvindt. Overigens is deze situatie ook voor de politie zelf niet wenselijk. Er is immers het risico van een versnipperde aanpak van terrorisme.

Onder de nationale politie zal afstemming zoals gezegd makkelijker worden. Dit is weliswaar nog geen oplossing voor het door ons geconstateerde gebrek aan vertrouwen, maar het is wel een verbetering in de zin dat het voor alle partijen overzichtelijker wordt als er één duidelijk aanspreekpunt en gesprekspartner is voor de politie. Voor de CIE van de landelijke eenheid zal dit overigens wel betekenen dat zij, nog meer dan in de huidige situatie het geval is, moet gaan runnen op terrorisme. Dit vereist een zekere inspanning op het gebied van capaciteit. Voorts zal dit ook aanpassing behoeven van runners: uit ons onderzoek blijkt namelijk dat onderzoeken naar terrorisme een hele andere dynamiek hebben en andere eisen stelt aan runners dan de commune criminaliteit. Overigens wordt in ontwerpplan ook specifiek gewezen op het belang van afstemming tussen de landelijke eenheid en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) (Ontwerpplan Nationale Politie 2011: 44; 56; 101). Wellicht dat de NCTV in de toekomst een soort ‘spelverdeler’ zal worden tussen de AIVD en de politie als het gaat om de aanpak van terrorisme. Evenals bij andere ontwikkelingen met betrekking tot de nationale politie, is het echter nog te vroeg om hierover uitspraken te doen.

Een tweede aspect van de nationale politie dat van belang is voor de verhouding tussen de AIVD en de politie betreft de RID. In de huidige situatie zijn alle medewerkers van de RID zogenoemde ‘artikel-60 ambtenaren’ die zowel onderzoeken uitvoeren op het gebied van de WIV als openbare orde. In de nationale politie zal er een scheiding worden aangebracht tussen beide taken en is er sprake van een WIV-team en een openbare orde-team. Het WIV-team zal grotendeels (bestuurlijk en in termen van gezag) onder de AIVD vallen, en het team dat is belast met de openbare orde valt dan helemaal onder de politie. Formeel juridisch is dit al het geval, en de organisatorische scheiding brengt de praktijk hiermee meer in overeenstemming. En ook de dubbele-petten problematiek behoort hiermee tot het verleden. Al met al lijkt dit een positieve ontwikkeling. Echter, omdat de WIV-teams helemaal los komen te staan van de politie, zou dit kunnen leiden tot een grotere afstand tussen deze teams en de rest van de politie. Zij zijn immers in alle opzichten onderdeel van de AIVD geworden. De belangrijkste reden waarom zij bij de politie ondergebracht blijven, is de gemakkelijke toegang tot de politie-informatie. Dit geldt zowel voor het verkrijgen van informatie via de formele weg (door het bevragen van de politiesystemen) als voor de informele weg (hetgeen vaak sneller betere informatie oplevert). Wij vragen ons af of de nieuwe indeling van de RID een negatieve invloed heeft op het gebruik van de informele wegen voor de WIV-teams. Immers, ze lopen hetzelfde risico als de CT-infobox om vereenzelvigd te worden met de AIVD en daarmee minder (of niet) te worden vertrouwd. Overigens is het grote verschil dat ook

de WIV-teams een onderdeel zijn van de RIO en binnen de politie zijn gehuisvest, en niet (zoals bij de CT-infobox het geval is) bij de AIVD. Echter, ook hiervoor geldt dat de plannen onvoldoende zijn uitgewerkt om daadwerkelijk een voorspelling te doen. Wij laten het daarom hierbij.

9.7 Slotbeschouwing

Dit proefschrift vormt de neerslag van een onderzoek naar de implementatie van intelligence in de context van de opsporing en de invloed daarvan op de verhouding tussen de AIVD en de politie. De verwachting omtrent dit onderwerp was bij aanvang van het onderzoek dat IGP een belangrijke en verregaande verandering van het politiewerk inhield en dat dit mogelijk problemen zou opleveren met de rechtsstatelijke scheiding tussen de AIVD en de politie. Wij hebben in dit onderzoek echter betoogd dat de veranderingen in de praktijk minder ver gaan dan in theorie, en dat het met de verminderende scheiding tussen de AIVD en de politie ook meevalt.

Dit is echter een exploratief onderzoek, en zoals al het exploratieve onderzoek roept het uiteindelijk meer vragen op dan er beantwoord zijn. Desalniettemin zijn wij van mening dat wij in het onderzoek de complexiteit van het onderwerp hebben aangetoond en daarmee hebben laten zien dat discussies omtrent nieuwe opsporingsmethoden, inlichtingen- veiligheids- en politiediensten en intelligence vragen om extra onderzoek. Met name (1) het delen van informatie en geheimhouding, (2) de verandering van complexe bureaucratische organisaties als de politie en (3) de rol van vertrouwen in intra-organisationele relaties herbergen nog veel te ontdekken nieuwe problemen, relevante inzichten en mogelijke oplossingen voor de reeds bekende problemen.

Samenvatting

In ons onderzoek hebben we ons gericht op de implementatie van de intelligencegestuurde politie (IGP) in de praktijk van de Criminele Inlichtingeneenheid (CIE). IGP is een herijking van het politiebestel, een nieuw politieparadigma. Door middel van de implementatie van het concept intelligence in de context van de CIE moet de politie effectiever en efficiënter worden. Intelligence is echter afkomstig uit de wereld van de (inlichtingen- en) veiligheidsdiensten. In Nederland is de veiligheidsdienst AIVD strikt gescheiden van de opsporingsorganisaties, waaronder de CIE. Dit proefschrift beschrijft ons onderzoek naar (A) de praktijk van IGP bij de CIE en (B) de invloed van IGP op de verhouding tussen de AIVD en de CIE.

Ons onderzoek is een exploratief onderzoek waarbij we met name de praktijk van IGP en de verhouding tussen de AIVD en de CIE hebben behandeld. Het onderzoek kent een beschrijvend deel (hoofdstuk twee tot en met vijf) waarin wij een beeld schetsen van de door ons onderzochte organisaties en concepten. Daarnaast is er een empirisch deel (hoofdstuk zes tot en met acht) waarin we ingaan op de praktijk van dezelfde organisaties en concepten. Het empirische deel vormt voor het grootste deel het exploratieve element van het onderzoek.

In hoofdstuk één geven we centrale probleemstelling, de onderzoeksvragen en de belangrijkste definities. IGP definiëren wij als "*de implementatie van intelligence in de context van de CIE*". Vervolgens geven we een definitie van intelligence: "*de overkoepelende term voor de reeks van activiteiten – van het vaststellen van een inlichtingenbehoefte en het verzamelen van informatie tot analyse en verspreiding – die in het geheim plaatsvinden en die erop zijn gericht op het bewaken of vergroten van de veiligheid door middel van het geven van voorwaarschuwingen voor bedreigingen of potentiële bedreigingen op een manier die ruimte biedt voor een tijdige implementatie van een preventief beleid of strategie.*" Voorts komen we tot de volgende centrale probleemstelling.

PS: Wat zijn de gevolgen van de implementatie van het concept van intelligence in de context van de Nederlandse opsporing voor de verhouding tussen de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Criminele Inlichtingeneenheid (CIE) van de Nederlandse politie?

De probleemstelling leidt tot vier onderzoeksvragen. Deze vragen luiden als volgt.

OV 1: Wat zijn de traditionele kenmerken van veiligheidsdiensten en de politie?

OV 2: Wat is het concept IGP en hoe beoogt dit concept de traditionele Nederlandse CIE te veranderen?

OV 3: In hoeverre is IGP geïmplementeerd in de Nederlandse CIE-praktijk?

OV 4: Wat is de verhouding tussen de AIVD en de CIE in de praktijk?

Tot slot geven we in hoofdstuk één een introductie van onze methode van onderzoek: de etnografie. In een exploratief onderzoek als de onze is de etnografie de aangewezen methode van onderzoek. We begeven ons in de praktijk van het

intelligence-werk, en aan de hand van literatuuronderzoek, interviews en participerende observatie hebben wij onze data verzameld. Omdat ons empirisch onderzoek bij de CIE/RIO heeft plaatsgevonden, beantwoorden wij de probleemstelling en de onderzoeksvragen vanuit het politieperspectief. Wij hebben slechts een beperkt inzicht gekregen in de relevante gerelateerde (interne) ontwikkelingen bij de AIVD.

Hoofdstuk twee behandelt de eerste onderzoeksvraag. We proberen inzicht te verschaffen in de verschillen tussen de traditionele veiligheidsdiensten en de politie. Deze verschillen bespreken we aan de hand van de theoretische modellen van de hoge politie en de lage politie. Ten eerste stellen we vast dat de veiligheidsdienst zich richt op de nationale veiligheid (HP-kenmerk 1) en de politie op de opsporing van criminaliteit (LP-kenmerk 1). Ten tweede constateren we dat de veiligheidsdienst werkt met voorwaarschuwingen en de daarvoor noodzakelijke opbouw en instandhouding van een informatiepositie (HP-kenmerk 2), en de lage politie zich richt op de materiële strafprocesrechtelijke waarheidsvinding door middel van het zoeken van bewijs omtrent datgene wat reeds is gebeurd (LP-kenmerk 2). Ten derde stellen we dat de hoge politie werkt volgens het werkproces van intelligence (HP-kenmerk 3), terwijl de lage politie werkt volgens het werkproces van opsporing (LP-kenmerk 3). Ten vierde constateren we een verregaande geheimhouding bij de hoge politie (HP-kemmerk 4), en (in de hoofdregel) transparantie bij de lage politie (LP-kenmerk 4).

In hoofdstuk drie beschrijven wij de Nederlandse veiligheidsdienst: de AIVD. Wij schetsen met name de juridische en organisatorische context van de AIVD, alsmede de interne structuur. De informatieverzameling, -verwerking, en -verstrekking door de AIVD wordt in verregaande mate gereguleerd door de WIV 2002. Voor de inzet van de bijzondere inlichtingenmiddelen geldt dat er een proportionaliteits- en subsidiariteitstoets dient plaats te vinden en er gelden bepaalde procedurele eisen. Op de verwerking van gegevens, die binnen de AIVD plaatsvindt, is door ons weinig zicht gekregen. Dit is echter anders in het geval van verstrekkingen van inlichtingen door de AIVD. De AIVD kent een zeer verregaande geheimhouding en de wijze waarop de dienst inlichtingen verstrekt, is zeer beperkt. Afnemers van AIVD-inlichtingen krijgen doorgaans een zeer summier ambtsbericht waar vrij weinig informatie in staat. Dit maakt de communicatie voor de AIVD met de buitenwereld erg lastig. Wanneer we de AIVD afzetten tegen de theoretische HP-kenmerken uit hoofdstuk twee, constateren dat deze ook opgaan voor de Nederlandse situatie. De AIVD is daarmee een typische hoge politie.

In hoofdstuk vier behandelen we de Criminele Inlichtingen Eenheid (CIE). We schetsen de historische ontwikkeling van de CIE en gaan in op de taak en werkzaamheden van de CIE. De CIE-taak is tweeledig en bevat (1) het runnen van informanten en (2) het verkrijgen van inzicht in de betrokkenheid van personen bij de zware en georganiseerde criminaliteit (de inzichttaak van artikel 10 lid 1 sub a Wpolg). Het runnen van informanten is voorbehouden aan de CIE: geen enkel ander onderdeel van de politie mag informanten runnen. Omdat het tweede deel van de CIE-taak voor een aanzienlijk deel door RIO's wordt uitgevoerd, beschouwen wij de RIO's voor dat deel als zijnde een onderdeel van de CIE. In de praktijk zijn veel regionale CIE-en overigens ondergebracht bij de RIO's. Voorts passen we de LP-

kenmerken toe op de CIE/RIO, en we constateren dat de CIE veel kenmerken van de traditionele lage politie heeft. De CIE is daarmee in belangrijke mate een lage politie.

In hoofdstuk vijf behandelen we het concept IGP en beantwoorden we OV 2. Wij beschrijven de achtergronden en uitgangspunten van het concept, en gaan uitgebreid in op de Nederlandse invulling van IGP.

We stellen vast dat IGP de politie dient te veranderen van een reactieve, incidentgestuurde organisatie in een intelligencegestuurde en proactieve organisatie. Criminaliteitsanalyse vormt de kern van IGP: de sturing dient op basis van geanalyseerde informatie plaats te vinden. Met behulp van IGP probeert de politie te reageren op de schaalvergroting waarmee zij in toenemende mate is geconfronteerd. IGP is vernieuwend omdat het een herziening is van het gehele politiebestel: het is in dat opzicht een verschuiving van het politieparadigma.

IGP verandert (in theorie) twee LP-kenmerken van de politie in HP-kenmerken. Allereerst legt IGP de nadruk op het geven van voorwaarschuwingen en de bijbehorende opbouw en instandhouding van een informatiepositie (HP-kenmerk 2). Daarnaast gaat IGP uit van het werkproces van de intelligence-cyclus (HP-kenmerk 3). Op het gebied van de taak (HP/LP-kenmerk 1) en de relatie met externen (HP/LP-kenmerk 4) stellen wij vast dat er vanwege de implementatie van IGP nauwelijks veranderingen op zijn getreden. Wij concluderen dat de implementatie van IGP de scheiding tussen de AIVD en de CIE lijkt te verkleinen.

In hoofdstuk zes beschrijven wij hoe we ons veldwerkonderzoek hebben uitgevoerd. Het hoofdstuk geeft een verdieping van de door ons gehanteerde onderzoeksmethode. We gaan uitgebreid in op de belangrijkste wijzen van dataverzameling, te weten literatuuronderzoek, interviews en participerende observatie. Van de interviews geven we aan wie we wanneer hebben geïnterviewd. Daarnaast behandelden we de belangrijkste stageafspraken betreffende geheimhouding en uiteindelijke publicatie. Tot slot geven we de lezer een impressie van hoe het onderzoek in de praktijk vorm heeft gekregen door enkele relevante momenten van het veldwerk te beschrijven. We beschrijven de mate waarin we (voor zover we zelf kunnen vaststellen) werden geaccepteerd en de eerste indrukken die de stageorganisatie op ons als onderzoeker achter heeft gelaten.

Hoofdstuk zeven is het meest omvangrijke hoofdstuk. Het hoofdstuk vormt een belangrijk deel van onze empirische onderzoek. Hier behandelen wij de praktijk van de implementatie van IGP en geven we antwoord op OV3. We beoordelen in hoeverre de CIE/RIO's erin zijn geslaagd om hun eigen uitwerking van IGP (het NIM) te implementeren. Wij concluderen dat (1) er in de praktijk sprake is van tekortschietende sturing, (2) de informatieverzameling grotendeels reactief is en (3) de informatieverwerking wordt bemoeilijkt door falende informatiesystemen en tekortschietende informatieprocessen. Dit betekent dat er, op het moment van onderzoek (2007-2011), in de praktijk bij de door ons onderzochte organisatieonderdelen nauwelijks sprake is van IGP. Wij betogen dat er drie overkoepelende redenen zijn die onzes inziens aan de falende implementatie van IGP ten grondslag liggen, te weten (1) onduidelijkheid omtrent IGP en wat het concept beoogt te bereiken, (2) hardnekkige structuurkenmerken van de politie die implementatie van elementen van IGP bemoeilijken en (3) de weerbarstige politiecultuur die zich moeilijk laat veranderen.

Met betrekking tot (1) constateren wij dat er met betrekking tot het begrip IGP sprake is van een verregaande *netwidening* waardoor op de werkvloer (en daarbuiten) onduidelijk is wat er precies onder IGP wordt verstaan.

Met betrekking tot (2) benoemen wij de drie meest hardnekkige structuurkenmerken die onzes inziens de belangrijkste rol spelen bij het belemmeren van IGP: (A) een tekortschietende ICT-infrastructuur, (B) een *street-level bureaucracy* organisatie die *top-down* sturing tegenwerkt (zo niet onmogelijk maakt) en (C) een verregaande concurrentie tussen verschillende afdelingen.

Met betrekking tot (3) benoemen wij drie weerbarstige cultuurkenmerken die de implementatie van IGP in de weg staan: (A) de medewerkers van de CIE (en in mindere mate de RIO) zijn conservatief en niet snel geneigd om mee te gaan in veranderingen, (B) er heerst een verregaande waan-van-de-dag-denken en (C) binnen de CIE is sprake van een cultuur van geheimhouding.

Wij concluderen dat IGP pas succesvol kan worden geïmplementeerd indien de problemen die voortvloeien uit de redenen worden opgelost.

Hoofdstuk acht beantwoordt OV 4. In dit hoofdstuk betogen we dat de verhouding tussen de AIVD en de CIE/RIO nog steeds meer kenmerken heeft van concurrentie dan van samenwerking. We stellen dat de drie van de vier door ons benoemde verschillen tussen de hoge politie (AIVD) en de lagen politie (CIE/RIO) in theorie steeds kleiner zijn geworden. Het gaat om veranderingen in (1) taak, (2) middel en (3) werkproces. Voorts zien wij ook veranderingen in (4) aandachtsgebied. Voor al deze gebieden geldt dat de politie steeds meer de kant opschuift van de hoge politie. Ze onderzoekt zaken van nationaal belang, geeft voorwaarschuwingen, implementeert het werkproces van de intelligence-cyclus en richt zich op het taakgebied van terrorisme. Omdat de politie (en dus de CIE/RIO) in toenemende mate naar de AIVD opschuift, zijn er voor beide organisaties voldoende aanleidingen om de onderlinge interactie te verbeteren. Wij behandelen drie modaliteiten van interactie, die elk een (oplopende) gradatie van vertrouwen vereisen. Het gaat om (1) onderlinge afstemming van activiteiten, (2) structurele informatie-uitwisseling, en (3) daadwerkelijke samenwerking.

Om het vertrouwen tussen de organisaties te kunnen analyseren, sluiten wij aan bij de conceptuele benadering van vertrouwen van Hardin (2005). In deze benadering kent vertrouwen drie elementen: (1) een driehoeksrelatie tussen twee partijen A en B en datgene waarmee ze elkaar vertrouwen X waarbij er tussen A en B geen verschil in hiërarchie bestaat, (2) een reden voor vertrouwen (*incentive*) en (3) het risico dat het vertrouwen wordt geschonden. Wij betogen dat de eerste twee 'ingrediënten' van vertrouwen in voldoende mate aanwezig zijn in de relatie tussen de AIVD en de CIE/RIO. Ten eerste staan de organisaties niet in een materiële hiërarchische verhouding tot elkaar. Formeel is er weliswaar sprake van een hiërarchie (de AIVD staat 'boven' de politie), maar in de praktijk heeft de CIE/RIO, en zeker de CIE, voldoende mogelijkheden om deze hiërarchie te doorbreken. Ten tweede hebben de AIVD en de CIE/RIO genoeg operationele en politieke redenen om een duurzame relatie op te bouwen en in stand te houden. Doen ze dat niet, dan lopen beide partijen het risico dat de ander bepaalde onderzoeken doorkruist en wellicht frustreert. Wij stellen echter ook vast dat vanwege de verregaande geheimhouding van beide partijen het risico om elkaar daadwerkelijk te vertrouwen (het derde element van vertrouwen) te groot is. De CIE/RIO kan er niet op vertrouwen dat de AIVD haar belangen behartigt omdat zij dit, vanwege de geheimhouding, niet kan inschatten. Voor de AIVD geldt nog steeds het risico dat aan de politie verstrekte

informatie met teveel mensen wordt gedeeld, zeker indien er volgens het *need to share*-denken wordt gehandeld. Desondanks constateren wij in de praktijk wel stappen worden gezet in de richting van meer interactie, wellicht omdat het tweede element van vertrouwen (de *incentive*) vanwege externe (politieke en maatschappelijke) druk zeer groot is.

Omdat het ontbreken van vertrouwen sterker speelt naarmate de interactie intensiever wordt, stellen wij vast dat de eerste modaliteit van interactie, de onderlinge afstemming van werkzaamheden, in de praktijk redelijk tot goed verloopt. Het behoud van invloed en autonomie gecombineerd met de kleinschaligheid van net overleg maakt dat het in de praktijk vrij goed loopt en men doorgaans positief oordeelt over het overleg. Met betrekking tot de tweede modaliteit van interactie, de structurele informatie-uitwisseling, constateren we dat het met betrekking tot een deel van de CIE-informatie stroever verloopt. Vanuit de CIE is er terughoudendheid om de 00, 200 en 300 informatie te verstrekking omdat de informatie aan een anonieme partij (de AIVD) wordt verstrekt, en wat er verder met de informatie wordt gedaan is niet in te schatten. De laatste modaliteit (samenwerking) vergt nog meer openheid en onderlinge vertrouwen. De CT-infobox is een eerste poging tot daadwerkelijke verregaande samenwerking. Bezien vanuit het oogpunt van samenwerking beoordelen wij het evenwel niet als een succes. Voor politiemensen is de CT-infobox een onderdeel van de AIVD, waardoor er niet gesproken kan worden van daadwerkelijke samenwerking tussen de AIVD en de politie. De CT-infobox is bezien vanuit het oogpunt van een effectieve terrorismebestrijding wel succesvol. Het zorgt ervoor dat informatie gecombineerd kan worden geanalyseerd en dat er adviezen naar de bij terrorismebestrijding betrokken partijen wordt gestuurd. Daadwerkelijke samenwerking kan echter pas worden bereikt indien er meer sprake is van gelijkwaardigheid en de betrokken partijen niet meer vallen onder verantwoordelijkheid en aansturing van de AIVD.

Wij concluderen dat de verhouding tussen de AIVD en de CIE/RIO in de praktijk nog steeds weinig kenmerken van een vertrouwensrelatie heeft. Dit zal zo blijven totdat aan alle voorwaarden van vertrouwen wordt voldaan.

In hoofdstuk negen formuleren wij onze antwoorden op de onderzoeksvragen en de probleemstelling. Wij betogen dat er een causaal verband is tussen (de implementatie van) IGP en de belangrijkste veranderingen die optreden in de verhouding tussen de AIVD en de CIE/RIO. IGP is vanuit het perspectief van de politie (CIE/RIO) het conceptuele raamwerk waarbinnen de veranderingen optreden. De door ons geconstateerde verschuivingen van LP- naar HP-kenmerken kunnen voor een groot deel worden verklaard met behulp van het concept IGP. Zeker wanneer het LP-kenmerk twee en drie betreft is het causale band duidelijk. Kenmerken één en vier beïnvloeden IGP indirect of worden indirect door IGP beïnvloed. Door de beoogde implementatie van IGP worden de verschillen tussen de AIVD en de CIE/RIO steeds kleiner, althans in theorie. Dat de implementatie van IGP in de praktijk maar moeizaam verloopt, laat onverlet dat er in de perceptie van beide organisaties steeds meer noodzaak bestaat om onderling af te stemmen. Deze noodzaak zal toenemen naarmate IGP verder wordt geïmplementeerd. Voor zowel de AIVD als de CIE/RIO (en de politie in het algemeen) geldt dan ook dat er moet worden geïnvesteerd in de onderlinge interactie en het opbouwen van vertrouwen.

Summary

In the Netherlands, national security intelligence is strictly separated from law enforcement. Our research deals with the relation between the security services (known by their Dutch acronym AIVD) and the Dutch criminal intelligence units (known by their Dutch acronym CIE). The focus of our research is the influence of the implementation of intelligence-led policing (ILP) on the separation between the two organizations AIVD and CIE.

Because of the secrecy imposed, empirical research into the security services and law enforcement is scarce. Therefore our research is exploratory. The research is divided into a descriptive part (chapters two to five), in which we describe the relevant organizations and concepts using the existing literature as a primary data-collection method, and an exploratory empirical part (chapters six to eight), which concentrates on these organizations and concepts in practice using interviews and participating observation as data-collection method.

Chapter one contains the most important definitions, our problem statement and research questions. Two definitions are as followed. We define ILP as "*the implementation of intelligence in the context of law enforcement*". Then we define intelligence, using Gill and Phythian's definition (2006: 7): "(intelligence is) *the umbrella term referring to the range of activities- from planning and information collection to analysis and dissemination- conducted in secret, and aimed at maintaining or enhancing relative security by providing forewarning of threats or potential threats in a manner that allows for the timely implementation of a preventive policy or strategy (…).*" Now we arrive at our central problem statement (PS):

PS: What are the consequences of the implementation of the concept of intelligence in the context of Dutch law enforcement for the relation between the security service (AIVD) and the criminal intelligence unit (CIE)?

The problem definition leads to the following four research questions.

1. What are the traditional characteristics of security services and law enforcement?
2. What is the concept of ILP and how does this concept supposedly change the traditional CIE?
3. To what extent has ILP been implemented in the CIE?
4. What is the actual relation between the AIVD and the CIE?

Chapter one concludes by a description of our research method: the ethnography. For an exploratory research such as ours, the ethnography proved to be most useful.

Chapter two answers the first research question. Using Brodeur's (2007) theoretical model of high policing (HP) and low policing (LP), we try to provide insight into the differences between the traditional security service and traditional law enforcement. First, we find that the security services traditionally focus on issues of national security. Politically motivated forms of violence, such as terrorism, fall within their scope of operations (HP-characteristic 1). In contrast, law enforcement traditionally focuses on crime, and the political aspects of terrorism fall outside of its scope of operations (LP-characteristic 1). Second, we find that the security services aim to

provide timely forewarnings of possible threats to national security (HP-characteristic 2). Law enforcement traditionally tries to establish the truth by collecting evidence regarding to criminal acts that took place in the past (LP-characteristic 2). Third, we find that the security services work according to the intelligence cycle, a demand-driven process in which information is first collected, then processed, analyzed and disseminated (HP-characteristic 3). Law enforcement works according to the process of the criminal investigation, a case-driven working process in which evidence becomes part of a case file (LP-characteristic 3). Fourth, the security services (for obvious reasons of security) uphold far-going secrecy (HP-characteristic 4). Law enforcement however should primarily be transparent in order to comply with the provisions and principles of a fair trial (LP-characteristic 4).

Chapter three describes the legal and organizational context and internal structure of the AIVD. The AIVD is primarily tasked with protecting national security, and to this end has extensive means and methods. The collection, processing and dissemination of intelligence is regulated by the Security and Intelligence Services Act of 2002 (known by its Dutch acronym WIV 2002). Collecting intelligence can take place using certain so-called 'special intelligence means', including HUMINT. We were not able to describe the processing and analysis of intelligence by the AIVD, as protecting these methods fall within the extensive scope of secrecy. We did describe the dissemination of intelligence. Because of provisions of secrecy, recipients of intelligence usually have to settle for brief and formal documents containing little information, aside from the strictly necessary factual statements. This makes the communication of the AIVD with other parties such as the CIE quite problematic.

When we compare the AIVD with the theoretical HP-characteristics, we find that all of these apply to the AIVD, making the AIVD a typical high policing agency.

Chapter four describes the CIE, starting with its history, task and operations. The task of the CIE is twofold: (1) the handling of informants and (2) gaining insight into serious and organized crime. Informant-handling is exclusively reserved for the CIE. Because of security reasons (the informants life is at stake if his role as an informer gets out), the CIE is separated from other parts of law enforcement and upholds far-going secrecy. This secrecy hinders communication with other parts of the police organization and external parties. Regarding the second part of the task of the CIE, we find that this is primarily performed by the Regional Information Organization (RIO). As far as relating to the analysis of organized crime we therefore consider the RIO to be a part of the CIE. The chapter concludes by finding that the CIE has three out of four of the LP-characteristics (missing LP-characteristic four, namely transparency), making it a low policing agency.

Chapter five analyzes the concept of ILP, describing ILP's background, objectives and the specific Dutch approach to ILP.

Within law enforcement, ILP is primarily regarded as a managerial model that is meant to transform law enforcement from a reactive organization into a proactive and preventive organization. Crime-analysis is at the core of ILP. ILP is a new concept in the sense that it offers law enforcement a method through which it can deal with (1) the netwidening of criminal law and (2) the immense increase in (both internal and external) information flows that that need to be managed.

In theory, ILP changes a low police into a high police. First, ILP (partly) shifts law enforcement towards providing forewarnings of possible (criminal) threats (HP-characteristic 2). Second, ILP centralizes around the process of the intelligence cycle (HP-characteristic 3). Third, regarding the task (LP-characteristic 1) and the relation with external partners (LP-characteristic 4) we find very little changes. However, there is a big shift in the scope of law enforcement, especially related to terrorism investigations (HP-characteristic 1). We therefore conclude that the implementation of ILP decreases the separation of the AIVD and the CIE.

Chapter six describes our field work and research method, the ethnography. For a period of two and a half years we conducted our fieldwork participating in an intelligence team of a RIO and later a CIE. We give an in-depth account of our primary methods of data collection, namely literature research, interviews and participating observation. As regards the interviews, we describe whom we interviewed and when these interviews took place. We also describe the most important provisions regarding the agreement with the organization where our fieldwork took place. There could not be any censorship by the organization, but they did have the right to postpone publication for a period of six months. Furthermore, we agreed not to publish any information that might jeopardize on-going investigations.

We conclude the chapter by describing the extent to which we were prone to the process of 'going native'. We cannot deny that, at first glance, going native applies to our situation to some extent. However, we believe we have limited the negative consequences of going native by (1) keeping a journal in which we extensively described and questioned the nature of going native and the possible impact it might have on our research and (2) extensively discussing this possible problem with the professors. In the end, we believe that we did not go native in the sense that we remained objective and did not over-identify with the police organization.

Chapter seven describes the findings of our exploratory fieldwork. We describe the extent to which the CIE has succeeded in implementing ILP. Our findings are threefold: (1) managing the activities of the CIE falls short to the requirements of ILP, (2) the collection of information remains highly reactive and (3) processing information is hampered by failing information systems and the shortcomings in informational processes. This means that in the period that we conducted our research (2007-2011), the Dutch law enforcement (especially the CIE) had yet to become truly intelligence-led. We identify three main causes for the (up to that point) failing implementation of ILP. These are (1) the ambiguity with regard to the meaning and definition of ILP, (2) the structural characteristics of law enforcement organizations form a barrier to the implementation of ILP and (3) the police culture proves to resist the necessary changes.

Regarding (1) we find that ILP is subject to far-going netwidening which creates a great deal of confusion and vagueness on the work floor regarding to what should and what should not fall under the definition of ILP.

Regarding (2) we name three deeply rooted structural problems that prevent an adequate implementation of ILP: (A) a failing ICT-infrastructure, (B) a street-level bureaucracy that prevents top-down management and (C) far-going competition between different parts of the law enforcement community.

Regarding (3) we name three aspects of police culture that prove to be especially problematic: (A) the CIE (and to a lesser extent the RIO) is conservative and resists change, (B) there is a pervasive day-to-day mentality that prevents proactivity and (C) there is a so-called culture of secrecy, especially regarding to the CIE.

Thus, we may conclude that ILP can only be implemented successfully if the underlying main reasons for these problems are addressed.

Chapter eight answers research question four. We find that three differences between the AIVD and the CIE/RIO theoretically have become smaller. The CIE/RIO (1) investigates cases related to national security by shifting its focus to anti-terrorism operations, (2) provides forewarnings of threats and (3) implements the intelligence cycle as leading work process. Because of this increasing, both AIVD and CIE/RIO should have sufficient incentives to improve their interaction. The potential risk to operational activities is simply too high to ignore. To interact constructively, there should be some form of trust between these organizations.

In order to analyze the trust-relation between these organizations, we use Hardin's (2005) conceptual approach of trust as encapsulated interests. This approach distinguishes three key-elements of trust, namely (1) a three-part relation between parties A and B and the subject of trust X in which the relation is based on equality instead of hierarchy, (2) an incentive and (3) a certain risk, namely the chance that the other party might turn out not to have been trustworthy. We state that the first two elements of trust are present in the relation between the AIVD and the CIE/RIO. First, there is no factual hierarchy between the organizations. There is a formal hierarchy that places the AIVD above the CIE/RIO, but in reality the latter party has sufficient possibilities to circumvent this formal hierarchy. Second, both the AIVD and the CIE/RIO have operational and political incentives to establish an enduring and stable relation and trust each other. The problem lies in the third element of trust: risk. Because of the far-going secrecy both organizations cannot adequately assess whether or not their interests are being met by the other organization. In other words: this secrecy makes it virtually impossible for security services and law enforcement to trust one another. Despite the risk, we find that both organizations do try to establish more interaction, probably because of the external pressure (the incentive).

We describe three modes of interaction which require an increasing amount of trust. These are (1) the adjusting of activities, (2) structural information exchange and (3) factual operational cooperation. We find that the first form is quite successful in practice. The AIVD and the CIE/RIO have frequent meetings regarding to operational cases and activities. Both organizations keep their autonomy and influence, and this (combined with the fact that it is a small-scale meeting) makes that it is considered successful and important. Regarding the second modality of interaction we find that this is more problematic, especially with regard to the most sensitive CIE-information. Sharing information with the AIVD turns out problematic for the CIE because they cannot assess in what way their information is used by the AIVD. This is too big of a risk for the CIE. The third modality of interaction is even more problematic. In theory far-going cooperation takes place within the so-called Counter-Terrorism Information Box (CT-Infobox). This is an organization in which different parties that are involved in counter-terrorism share and analyze all relevant information. From a counter-terrorism perspective, the CT-infobox has a significant contribution to the effectiveness of operational activities. In this regard it is without question a success. However, from a cooperation perspective the CT-infobox is not a success. According to employees of the CIE/RIO, there is no difference between the

AIVD and the CT-infobox. The latter is physically, organizationally and legally positioned as part of the AIVD. Therefore the trust-related issues mentioned above also arise between the CIE/RIO and the CT-infobox. One can only speak of true cooperation and trust when there is equality between both parties, and this can only be achieved when the CT-infobox is separated from the AIVD.

Thus, we may conclude that the relation between the AIVD and the CIE/RIO in practice cannot be characterized as one of trust. This will remain as long as the elements of trust are not met.

In chapter nine we formulate our answers to the research questions and problem definition. We argue that there is a causal relation between the implementation of ILP and the most important changes in the relation between the AIVD and the CIE/RIO. From a law-enforcement (CIE/RIO) perspective, ILP is the conceptual framework in which most change takes place. The shift from LP-characteristics towards HP-characteristics can (for a large part) be explained using the concept of ILP. Especially the changes into HP-characteristic 2 (the forewarning of threats) and HP-characteristic 3 (the intelligence cycle) are directly related to ILP. LP-characteristic 1 (the focus on crime) and LP-characteristic 4 (transparency) are indirectly influenced by ILP or influence ILP indirectly. Overall, because of the implementation of ILP the differences between the AIVD and the CIE/RIO theoretically diminish. Notwithstanding the fact that this implementation meets considerable difficulties, the AIVD and CIE/RIO increasingly need to adjust their activities to one another. This necessity will increase as ILP gets further implemented. Both the AIVD and the CIE/RIO (and law enforcement in general) therefore need to invest more in gaining each other's trust and improve their interaction. Without this investment their interaction will continue to suffer the negative consequences of a lack of trust and can be characterized as competitive.

Referenties

Aalbersberg, Barendregt en De Wit 1993
P.J. Aalbersberg, B.N. Barendregt en J.B.A. de Wit, "De ontwikkeling van het CID-werk." In *Criminele inlichtingen: de rol van Criminele Inlichtingendiensten bij de aanpak van de georganiseerde misdaad*, door A.W.M. van der Heijden, 's-Gravenhage, VUGA Uitgeverij, 1993, p. 50-65.

Aalberts 2009
T.E. Aalberts, "Een gevaarlijke driehoeksverhouding? Falende staten, georganiseerde misdaad en transnationaal terrorisme." In: *Juridische Verkenningen*, 35 (3), 2009. p. 13-30.

Aardema 2008
H. Aardema, *Politieleiderschap: verbinding bovenstroom en onderstroom*, Politieacademie, 2008.

Abels en Willemse 2004
P.H.A.M. Abels en R. Willemse, "Veiligheidsdienst in Verandering: de BVD/AIVD sinds het einde van de Koude Oorlog." In: *Justitiële Verkenningen (WODC)*, 2004, p. 83-98.

Abels 2007
P. Abels, "'Je wilt niet geloven dat zoiets in Nederland kan!' Het Nederlandse contraterrorismebeleid sinds 1973." In: I. Duyvesteyn en B. de Graaf (red.), *Terroristen en hun bestrijders vroeger en nu*, Amsterdam, Boom, 2007, p. 121-128.

Adviescommissie Informatiestromen Veiligheid 2006
Adviescommissie Informatiestromen Veiligheid, *Data voor Daadkracht, Gegevensbestanden voor veiligheid: observaties en analyse.* Den Haag, Deltahage, 2006.

Aftergood 1999
S. Aftergood, "Government Secrecy and Knowledge Production: A Survey of some General Issues (1999)." In: S.L. Maret en J. Goldman, *Government Secrecy: classic and contemporary readings*, London, Libraries Unlimited, 2009, p. 296-304.

Algemene Rekenkamer 2005
Algemene Rekenkamer, *ICT bij de politie: terugblik 2005*, 's-Gravenhage, 2005.

Algemene Rekenkamer 2011
Algemene Rekenkamer, "ICT Politie 2010." 's-Gravenhage, 2011.

Andreas en Nadelmann 2006
P. Andreas en E. Nadelmann, *Policing the Globe: criminalization and crime control in international relations.* New York, Oxford University Press, 2006.

Baron, Byrne en Johnson 1998
R.A. Baron, D. Byrne en B.T. Johnson, *Exploring Social Psychology.* Needham Heights, Allyn and Bacon, 1998.

Bartell en Dutton 2001
C. Bartel en J. Dutton, Ambiguous Organizational Memberships: Constructing Organizational Identities in Interactions With Others. In: M.A. Hogg en D.J. Terry (ed.), *Social Identity Processes in Organizational Contexts*, Philadelphia, Psychology Press, 2001, p. 115-130.

Bayley 2005
D.H. Bayley, "What do the police do?" In: T. Newburn (ed.), *Policing: Key Readings*, Devon, Willan Publishing, 2005, p.141-149.

Beck 1992
U. Beck, *The risk society: towards a new modernity.* London, Sage, 1992.

Beijer et al. 2004
A.Beijer, R.J. Bokhorst, M. Boone, C.H. Brants en J.M.W. Lindeman, *De Wet bijzondere opsporingsbevoegdheden - eindevaluatie.* Meppel, Boom Juridische Uitgevers, 2004.

Van der Bel, Van Hoorn en Pieters 2009
D. van der Bel, A.M. van Hoorn en J.J.T.M. Pieters, *Informatie en Opsporing: Handboek informatieverwerving-, verwerking en - verstrekking ten behoeve van de opsporingspraktijk*, Zeist: Kerckebosch, 2009.

Benveniste 1998
G. Benveniste, "Survival inside bureaucracy." In: G. Thompson, J. Frances, R. Levacic en M. Jeremey (ed.), *Markets, Hierarchies & Networks: the coordination of social life*, London, Sage Publications, 1998, p. 141-153.

Besse en Kuys 1997
A. Besse en J. Kuys, *Cowboys aan het Spaarne: Het IRT en de Strijd tegen de Zware Misdaad*, Breda, Uitgeverij De Geus, 1997.

Beumer et al. 2006
R.J. Beumer, W.M. van Andel, A.E.J.M. van Erp, L.J.M. Koolen en A.A.J. van der Meer, *Opsporing bezocht: rapportage over de eerste fase van het onderzoek naar de kwaliteit van de politiële opsporing*, Den Haag, IOOV, 2006.

Bittner 2005
E. Bittner, "Florence Nightingale in pursuit of Willie Sutton: a theory of the police." In: Tim Newburn, *Policing: Key Readings*, Devon, Willan Publishing, 2005, p. 150-172.

Blank 2008
L. Blank, "Two schools for secrecy: defining secrecy from the works of Max Weber, Georg Simmel, Edward Shils and Sissela Bok ." In: S.L. Maret en J. Goldman (eds.), G*overnment Secrecy: classic and contemporary readings (2008)*, London: Libraries Unlimited, 2009, p. 59-68.

Boeije 2006
H. Boeije, "Kwalitatief Onderzoek." In: H. 'Hart, H. Boeije en J. Hox, *Onderzoeksmethoden*, Boom Onderwijs, 2006, p. 253-289.

Bogard 2006
W. Bogard, "Surveillance assemblages and lines of flight." In: David Lyon (ed.), *Theorizing Surveillance: The panopticon and beyond*, Devon, Willan Publishing, 2006, p. 97-122.

Van den Bogert, Horsten en Tamerus 2008
E. van den Bogert, P. Horsten en J. Tamerus. *Tegenhouden Ontrafeld.* Deventer: Kluwer, 2008.

Boin, Van der Torre en 't Hart 2007
R.A.Boin, E.J. Van der Torre en P. 't Hart, "Politieleiderschap: korpschefs op het breukvlak." In: C.J.C.F. Fijnaut, E.R. Muller, U. Rosenthal en E.J. van der Torre (red.), *Politie: Studies over haar werking en organisatie*, Deventer: Kluwer, 2007, p. 313-334.

Borgers 2007
M.J. Borgers, *De vlucht naar voren,* Den Haag, Boom, 2007.

Born en Wetzling
H. Born en T. Wetzling, "Intelligence accountability: challenges for parliaments and intelligence services." In: L.K. Johnon, *Handbook of intelligence studies*, New York: Routledge, 2007: 315-328.

Boutellier 2005
H. Boutellier, *De veiligheidsutopie: Hedendaags onbehagen en verlangen rond misdaad en straf*, Den Haag: Boom Juridische Uitgevers, 2005

Brodeur 2007
J.P. Brodeur, "Policing in Post-9/11 Times." In: *Policing*, 2007, volume 1: 25-37.

Van den Broek 2010
H. van den Broek, "Politie en Openbaar Ministerie: samen de opsporing vernieuwen?" In: N. Kop en P. Tops (red.), *Toestand en toekomst van de opsporing*, Apeldoorn: Politieacademie, 2010, p. 33-43.

Brown 2001
R. Brown, "Intergroup Relations." In: Miles Hewstone en Wolfgang Stroebe, *Introduction to Social Psychology*, Oxford: Blackwell Publishing, 2001, p. 479-515.

Brinkhoff 2009
S. Brinkhof, "Controle op de Criminele Inlichtingeneenheden", in: Delikt en Delinkwent 2009, 10, p. 112-139.

Brunsson 1989
N. Brunsson, "The Organization of Hypocrisy: talk, decision and actions in organizations", 1989. In: Harrie Aardema, *Politieleiderschap: verbinding bovenstroom en onderstroom*, Politieacademie, 2008.

Van de Bunt 2002
H.G. van de Bunt, "de onderste steen: enkele kanttekeningen bij het primaat van het strafrecht in de waarheidsvinding." In: *Justitiële Verkenningen (WODC)* 28 (2002), p. 8-15.

Van de Bunt et al. 2001
H. van de Bunt, C. Fijnaut en H. Nelen, *Post-Fort: Evaluatie van het strafrechtelijk onderzoek (1996-1999)*, Den Haag, Sdu Uitgevers, 2001.

BVD 1996
Jaarverslag Binnenlandse Veiligheidsdienst 1996, te downloaden van: http://www.aivdkennisbank.nl/downloads/cDU370_Downloads.aspx, gezien op 7 november 2011

BVD 1997
Jaarverslag Binnenlandse Veiligheidsdienst 1997, te downloaden van: http://www.aivdkennisbank.nl/downloads/cDU370_Downloads.aspx, gezien op 7 november 2011

BVD 1998
Jaarverslag Binnenlandse Veiligheidsdienst 1998, te downloaden van: http://www.aivdkennisbank.nl/downloads/cDU370_Downloads.aspx, gezien op 7 november 2011

BVD 1999
Jaarverslag Binnenlandse Veiligheidsdienst 1999, te downloaden van: http://www.aivdkennisbank.nl/downloads/cDU370_Downloads.aspx, gezien op 7 november 2011

BVD 2000
Jaarverslag Binnenlandse Veiligheidsdienst 2000, te downloaden van: http://www.aivdkennisbank.nl/downloads/cDU370_Downloads.aspx, gezien op 7 november 2011

CBP 2005
College Bescherming Persoonsgegevens, Advies over Wet Politiegegevens, 2005. Te downloaden van http://www.cbpweb.nl/downloads_adv/z2005-1359.pdf, gezien op 29 november 2011.

Van Calster en Vis 2008
P. van Calster en T. Vis. "Veranderingsprocessen bij politie: Intelligence-led Policing." In: *Panopticon* 29, nr. 2008.5, p. 68-86.

Van Calster, Roosma en Vis 2010(a)
P. van Calster, J. Roosma en T. Vis, "Intelligence-gestuurde politie vanuit een politieel cultuur perspectief." In: *Proces 89(3)*, 2010 (a), p. 177-192.

Van Calster, Roosma en Vis 2010
P. van Calster, J. Roosma en T. Vis, "Intelligence-gestuurde politie en sociale categorisatie." In: *Proces 89 (1)*, 2010, p. 17-29.

Chan 2005
J. Chan, "Changing police culture." In: Tim Newburn (ed.), *Policing: key readings*, Devon: Willan Publishing, 2005, p. 338-363.

Chapman 1970
B. Chapman, *Police State*, London, Pall Mall Press Ltd., 1970.

Cleiren en Nijboer
C.P.M. Cleiren en J.F. Nijboer, *Tekst & Commentaar Stravordering, 7e druk*, Deventer: Kluwer , 2007.

Colby 1976
W.E. Colby, "Intelligence Secrecy and Security in a Free Society", 1976. In: Susan L. Maret en Jan Goldman (eds.), G*overnment Secrecy: classic and contemporary readings (2008)*, London: Libraries Unlimited, 2009, p. 477-486.

Coles 2001
N. Coles, *It's not what you know- It's who you know that counts. Analysing serious crime groups as social networks.* British Journal of Criminology 41(4), 2001, p. 580-594.

Commissie Bestuurlijke Evaluatie AIVD 2004
Commissie Bestuurlijke Evaluatie AIVD, *De AIVD in verandering: Bestuurlijke Evaluatie*, Den Haag, Ministerie van Binnenlandse Zaken, 2004.

Commissie Havermans 2004
Commissie Havermans, "AIVD in verandering: Commissie Bestuurlijke Evaluatie AIVD." Bestuurlijke Evaluatie, 2004.

Cope 2004
N. Cope, "'Intelligence Led Policing or Policing Led Intelligence?': Integrating volume crime analysis into policing." In: *British Journal of Criminology*, Volume 44, issue 2 (2004), p. 188-203.

Corstens 2008
G.J.M. Corstens, *Het Nederlandse Strafproces, zesde druk*, Deventer: Uitgeverij Kluwer BV, 2008.

CPRGS 1997
Commission on Protecting and Reducing Government Secrecy, "Rethinking Classification: Better Protection and Greater Openness" 1997. In: S.L. Maret en J.

Goldman (eds.), G*overnment Secrecy: classic and contemporary readings (2008)*, London: Libraries Unlimited, 2009, p. 487-517.

Crijns, Van der Meij en Ten Voorde 2008
J.H. Crijns, P.P.J. van der Meij en J.M. ten Voorde (eds.), *De waarde van waarheid: opstellen over waarheid en waarheidsvinding in het strafrecht*, Den Haag: Boom Juridische Uitgevers, 2008.

CTIVD 2007
CTIVD, *Accountability of intelligence and security agencies and human rights*, Verslag internationaal symposium, 7 en 8 juni 2007, Den Haag: CTIVD, 2007.

CTIVD 2007
CTIVD, *Toezichtsrapport inzake het onderzoek van de Commissie van Toezicht naar de Contra-Terrorisme Infobox*, Toezichtsrapport, Den Haag: CTIVD, 2007.

CTIVD 2009
CTIVD, *Toezichtsrapport inzake de toepassing door de AIVD van artikel 25 WIV 2002 (aftappen) en artikel 27 WIV 2002 (selectie van ongericht ontvangen niet-kabelgebonden telecommunicatie)*, Toezichtsrapport, Den Haag: CTIVD, 2009.

CTIVD 2012
CTIVD, *Jaarverslag 2011-2012*, Den Haag: TCIVD, 31 maart 2012.

Curtis en Karazan 2002
G.E. Curtis en T. Karazan, *The Nexus among terrorists, narcotics traffickers, weapons proliferators, and organized crime in Western Europe*, Washington: Federal Research Devision, Library of Congress, 2002.

Custers 2004
B. Custers, *The Power of Knowledge: ethical, legal and technological aspects of datamining and group profiling in Epidemiology*, Nijmegen: Wolf Legal Publishers, 2004.

Van Daele en Vangeebergen 2006
D. van Daele en B. Vangeebergen. *Inlichtingendiensten en strafprocedure in Nederland, Duitsland en Frankrijk.* Antwerpen: Intersentia, 2006.

Van Daele et al. 2010
D. van Daele, T. Kooijmans, B. van der Vorm, K. Verbist en C.J.C.F. Fijnaut, *Criminaliteit en rechtshandhaving in de Euregio Maas-Rijn, Deel 3: De bestuurlijke aanpak van georganiseerde criminaliteit in Nederland en België*, Oxford-Antwerpen: Intersentia, 2010.

Dalkir 2005
K. Dalkir, *Knowledge Management in Theory and Practice*, Oxford: Elsevier Butterworth-Heineman, 2005.

Davenport en Prusak 1998
T.H. Davenport en L. Prusak, *Working Knowledge: How Organizations Manage What They Know*, Boston, Massachusetts: Harvard Business School Press, 1998.

Deacon 1974
R. Deacon, *A History of the Chinese Secret Service*, Plymouth: Clarke,Doble & Brendon Ltd., 1974.

De Haan 2004
J. de Haan, "ICT en samenleving." In: P. Schnabel, *In het zicht van de toekomst: Sociaal en Cultureel Rapport,* Den Haag: Sociaal en Cultureel Planbureau, 2004, p. 223-266.

De Hert en Vis 2005
P. de Hert en T. Vis. "Intelligence Led Policing in de Nederlanden. Terminologische, grondrechtelijke en organisatorische bedenkingen." In: Tom Van Den Broeck, Els Enhus, Frank Goegebuer, luc Valkenborg en Annelies Vanlandschoot (ed.), *Intelligence led policing. Definitie, reikwijdte en grenzen*, Brussel: Politeia, 2005, p. 57-71.

De Hert, Huisman en Vis 2005
P. de Hert, W. Huisman en T. Vis, "Intelligence led policing ontleed." In: *Tijdschrift voor Criminologie*, 2005, vol. 47 nr. 4, p. 365-375.

De Kleuver 2007
E.E. de Kleuver, "Prestatieafspraken met de politie: van kritiek naar waardering." In: C.J.C.F. Fijnaut, E.R. Muller, U. Rosenthal en E.J. Van der Torre (red.), *Politie: Studies over haar werking en organisatie*, Deventer: Kluwer, 2007, p. 213-234.

De Koning 2010
B. de Koning, *Operatie Blauw: Weg met de bureaucratie bij de politie,* Amsterdam: Uitgeverij Balans, 2010.

De Poot et al. 2004
C.J. De Poot, R.J. Bokhorst, P.J. Van Koppen en E.R. Muller, *Rechercheportret: Over dilemma's in de opsporing*, Alphen aan den Rijn: Kluwer, 2004.

De Vries 2002
G.H. de Vries, "Wat is waarheid? Een filosofische benadering." In: *Justitiële Verkenningen (WODC)* 28, nr. 2 02 (2002), p. 16-25.

Den Hengst-Bruggeling 2010
M. den Hengst-Bruggeling, *Informatierijk en toch kennisarm?* Apeldoorn: Politie Academie, 2010.

Dobbelaar en Koemans 2008
J. D. en M. K., "De criminele terroristische organisatie: mythe of werkelijkheid?" In: E.R. Muller, U. Rosenthal en R. de Wijk, *Terrorisme: Studies over terrorisme en terrorismebestrijding*, Deventer: Kluwer, 2008, p. 193-215.

Duyvesteyn en De Graaf 2007
I. Duyvesteyn en B. de Graaf (red.), *Terroristen en hun bestrijders: vroeger en nu.* Amsterdam: Boom, 2007

Eck en Spelman 2005
J.E. Eck en W. Spelman, "Who ya gonna call? The police as problem-busters." In: Tim N. (ed.), *Policing: Key Readings*, Devon: Willan Publishing, 2005, p. 412-427.

Engelen 1995
D. Engelen, *Geschiedenis van de Binnenlandse Veiligheidsdienst*, 's-Gravenhage: Sdu Uitgeverij Koninginnegracht, 1995.

Engelen 2007
D. Engelen, *Frontdienst: de BVD in de Koude Oorlog*, Amsterdam: Uitgeverij Boom, 2007.

Ericson 2005
R.V. Ericson, "The police as reproducers of order." T. Newburn (ed.), *Policing: Key Readings*, Devon: Willan Publishing, 2005, p. 215-246.

Ericson en Haggerty 1997
R.V. Ericson en K.D. Haggerty, *Policing the Risk Society*, Toronto: University of Toronto Press, 1997.

Ferrell en Hamm 1998
J. Ferrell en M.S. Hamm, *Ethnography at the edge: Crime, Deviance and Field Research*, Boston: Norht Eastern University Press, 1998.

Ferrell 1998
J. Ferrell, "Criminological Verstehen: Inside the Immediacy of Crime." In: J. Ferrell en M.S. Hamm (ed.), *Ethnography at the Edge: Crime, Defiance and Field Research*, Boston: North Eastern University, 1998, p.20-42.

Fijnaut en Moerland 2000
C. Fijnaut en H. Moerland, "Achtergronden, geschiedenis en praktijk van de criminaliteitsanalyse." In: H. Moerland en B. Rovers (ed.), *Criminaliteitsanalyse in Nederland*, 's Gravenhage: Elsevier Bedrijfsinformatie, 2000, p. 21-31.

Fijnaut 2004
C. Fijnaut, "Inlichtingendiensten in Europa en Amerika: de heroriëntatie sinds de val van de muur en 11 september 2001." In: WODC, *Justitiële Verkenningen*, 2004/03, p. 10-42.

Fijnaut 2006
C. Fijnaut, *De Geschiedenis van de Nederlandse Politie: een staatsinstelling in de maalstroom van de geschiedenis*, Amsterdam, Boom, 2006

Fijnaut 2010
C. Fijnaut, "Toestand en toekomst van de opsporing: Enkele persoonlijke waarnemingen aan de frontlinie en uit de ivoren toren." In: N. Kop en P. Tops (red.), *Toestand en toekomst van de opsporing*, Apeldoorn: Politieacademie, 2010, p13-22.

Fijnaut 2012
C. Fijnaut, *Het toezicht op de inlichtingen- en veiligheidsdiensten: noodzaak van krachtiger samenspel. De vertrekpunten en uitkomsten van een gespreksronde*, 2012. Te downloaden van: http://www.ctivd.nl/

Findlay 2008
M. Findlay, *Governing through Globalised Crime: Futures for international criminal justice*, Devon: Willan Publishing, 2008.

Funder 2003
A. Funder, *Stasiland. True Stories from Behind the Berlin Wall*, London: Granta Books, 2003.

Garell, Freilich en Chermak 2007
E. Mc Garell, J.D. Freilich en S. Chermak, "Intelligence-Led Policing as a framework for responding to terrorism." In: *Journal of Contemporary Criminal Justice* vol. 23 no. 2 (2007), p. 142-158.

Garland 2002
D. Garland, *The Culture of Control: Crime and Social Order in Contemporary Society*, Oxford: Oxford University Press, 2002.

Geertz 1973
C. Geertz, "The Interpretation of Cultures", 1973. In: T.H. Eriksen en F. Nielsen, *A History of Anthropology*, London: Pluto Press, 2001, p. 102-104.

Van Gestel et al. 2009
B. van Gestel, C.J. de Poot, R.J. Bokhorst en R.F. Kouwenberg, *De Wet opsporing terroristische misdrijven twee jaar in werking*, Den Haag: WODC, 2009.

Van Gestel, De Poot en Kouwenberg 2010
B. van Gestel, C.J. de Poot en R.F. Kouwenberg, *De Wet opsporing terroristische misdrijven drie jaar in werking*, Den Haag: WODC, 2010.

Gill 2000
P. Gill, *Rounding up the usual suspects: developments in contemporary law enforcement intelligence*, Burlington, VT: Ashgate Publishing & Co, 2000.

Gill en Phythian 2006
P. Gill en M. Phythian, *Intelligence in an Insecure World*, Cambridge: Polity Press, 2006.

Goldstein 1979
H. Goldstein, "Improving policing: a problem-oriented approach", 1979. In: *Crime and Delinquency*, 25 (2): 236-258.

Goldstein 2003
H. Goldstein, "On further developing problem-oriented policing: The most critical need, the major impediments, and a proposal", 2003. In: J. Knutson (ed.), *Problem-Oriented Policing: From Innovation to Mainstream*, New York, Criminal Justice Press: 13-47.

De Graaff en Wiebes 1998
B. de Graaff en C. Wiebes, *Villa Maarheeze: de geschiedenis van de inlichtingendienst buitenland*, Den Haag: Sdu Uitgevers, 1998.

Guidetti en Ratcliffe 2008
R. Guidetti en J.H. Ratcliffe, "State police investigative structure and the adoption of intelligence-led policing." In: *Policing: An International Journal of Police Strategies and Management*, Volume 31, issue 1 (2008): 109-128.

Haenen en Meeus 1996
M. Haenen en T.J. Meeus, *Het IRT moeras*, Uitgeverij Balans, 1996.

Hahn 1998
P. Hahn, *Emerging Criminal Justice: Three Pillars for a Proactive Justice System*, Thousand Oaks: Sage, 1998.

Hamm 2007
M.S. Hamm, *Terrorism as Crime: From Oklahoma City to Al-Qaeda and Beyond*, New York: New York University Press, 2007.

Hardin 2006
R. Hardin, *Trust*, Cambridge: Polity Press, 2006.

Haslam en Platow 2001
S. Alexander Haslam en Michael J. Platow, Your Wish is Our Command: The Role of Shared Social Identity in Translating a Leader's Vision into Follower's Action. In: M.A. Hogg en D.J. Terry (red.), *Social Identity Processes in Organizational Contexts*, Philadelphia: Pscychology Press, Taylor and Francis Group, 2001, p. 213-228.

Hedley 2007a
J. Hollister Hedley, "Analysis for strategic intelligence." In: L. K. Johnson (ed.), *Handbook for Intelligence Studies*, New York: Routledge, 2007, p. 211-226.

Hedley 2007
J. Hollister Hedley, "The Challenges of Intelligence Analysis." In: L.K. Johnson (ed.), *Handbook for Intelligence Studies*, New York: Routledge, 2007, p. 123-138.

Henseler 2010
J. Henseler, "E-Discovery: Op zoek naar de digitale waarheid." *Openbare Les,* Amsterdam: HVA Publicaties, 2010.

Van den Herik 1993
H.J. van den Herik, "Knowledge Based Systems." *Collegedictaat.* Maastricht University, 1993.

Heuer 1999
R.J. Heuer, *Psychology of Intelligence Analysis,* Washington: CIA Center for the Study of Intelligence, 1999.

Hirsch Ballin 2012
M.F.H. Hirsch Ballin, *Anticipative Criminal Investigation: Theory and Counterterrorism Practice in the Netherlands and the United States,* Den Haag, T.M.C. Asser Press, 2012.

Hoekstra 2004
F. Hoekstra, *In dienst van de BVD: Spionage en contraspionage in Nederland*, Amsterdam: Boom, 2004.

Hoogenboom 1994
A.B. Hoogenboom, *Het Politiecomplex*, Arnhem: Gouda Quint BV, 1994.

Hoogenboom 2000
A.B. Hoogenboom, *Schaduwen over Van Traa*, Den Haag: Koninklijke Vermande, 2000.

Hoogenboom 2009
B. Hoogenboom, *Spelers op zoek naar regels en scheidsrechters: Informatie Inwinning Openbare Orde door de Regionale Inlichtingendienst*, Apeldoorn: Politie en Wetenschap, 2009.

Horsten en Tamerus 2005
P. Horsten en J. Tamerus, *Tegenhouden ontrafeld*, Deventer: Kluwer, 2005.

Hudson 2003
B. Hudson, *Justice in the Risk Society*, London: Sage Publications, 2003.

Huisman et al. 2011
S. Huisman, P. Duijn, T. Vis en H. Ardon, "Voorkom mismatch tussen intelligence-proces en *criminele werkelijkheid*". In: Het Tijdschrift voor de Politie, jg. 73/nr.8/11.

Hulnick 2007
A.S. Hulnick, "What's wrong with the intelligence cycle?" In: L.K. Johnson, *Strategic Intelligence Volume 2: The Intelligence Cycle: the flow of secret information from overseas to highest councils of government*, London: Praeger Security International, 2007, p. 1-21.

IME Consult 1989
IME Consult, *Bedrijfskundig vooronderzoek recherche; eindrapport.* Nijmegen: IME Consult Organisatie Adviesbureau, 1989.

IOOV 2006
Inspectie Openbare Orde en Veiligheid, *Opsporing bezocht: rapportage over de eerste fase van het onderzoek naar de politiële opsporingstaak.* Den Haag: IOOV, 2006.

IOOV 2009
Inspectie Openbare Orde en Veiligheid, *Informatiegestuurde Politie*, Den Haag: IOOV 2009.

Jacobs 1998
B.A. Jacobs, "Researching Crack Dealers: Dilemma's and Contradictions." In: J. Ferrell and M.S. Hamm, *Ethnography at the Edge: Crime, Defiance and Field Research*, Boston: Northeastern University Press, 1998, p. 159-177.

Jansen 2001
H.A. Jansen, "Informatiegestuurde opsporing moet Nederland veroveren." In: *het Tijdschrift voor de Politie*, nr. 6 (2001), p. 11-15.

Jeffreys-Jones 2007
R. Jeffreys-Jones, *The FBI: A History*, London: Yale University Press, 2007.

Johnson 2007
L.K. Johnson, *Handbook of Intelligence Studies*, New York: Routledge, 2007.

Johnston 2005
R. Johnston, *Analytic Culture in the U.S. Intelligence Community: an Ethnographic Study*, Pittsburgh: Government Printing Office, 2005.

Jones en Newburn 2005
T. Jones en T. Newburn, "The transformation of policing? Understanding current trends in policing systems (2002)." In: T. Newburn (red.), *Policing: Key Readings*, Devon: Willan Publishing, 2005, p. 733-750.

Jörg en Kelk 2001
N.D. Jörg en C. Kelk, *Strafrecht met Mate*, Gouda: Gouda Quint, 2001.

Keegan 2003
J. Keegan, *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda*, London: Hutchinson, 2003.

Van Kempen en Van de Voort 2010
P.H.P.H.M.C. van Kempen & J. Van de Voort, Nederlandse antiterrorismeregelgeving getoetst aan fundamentele rechten: een analyse met meer bijzonder aandacht voor het EVRM, WODC, 2010.

Kempny en Bursztа 2005
M. Kempny en W.J. Burszta, "On the relevance of common sense for anthropological knowledge". In: K. Hastrup en P. Hervik (ed.), *Social Experience and Anthropological Knowledge*, London en New York: Routledge, 2005, p. 91-103.

Kielman 2010
H. Kielman, *Politiële gegevensverwerking en Privacy: naar een effectieve waarborging*, Leiden: E.M. Meijers Instituut, 2010.

Kleemans en De Poot 2008
E.R. Kleemans en C.J. De Poot, *Criminal Careers in organized crime and social opportunity structure.* In: European Journal of Criminology, 5:69, 2008.

Klerks 2001
P. Klerks, *The network Paradigm applied to criminal organisations: theoretical nitpicking or a relevant doctrine for investigations? Recent developments in the Netherlands.* In: Connections 24(30), 2001, p. 53-65.

Klerks 2007
P.P.H.M. Klerks, "De politiële beheersing en bestrijding van georganiseerde criminaliteit." In: C.J.C.F. Fijnaut, E.R. Muller, U. Rosenthal en E.J. van der Torre (red.), *Politie: Studies over haar werking en organisatie*, Deventer: Kluwer, 2007, p. 865-888.

Klerks 2007
P. Klerks, "Methodological aspects of the Dutch National Threat Assessment." *Trends in Organized Crime*, 2007, p. 91-101.

Klerks 2010
P. Klerks, "Visie op opsporing: richtinggevend document voor criminaliteitsbeheersing en recherchewerk in praktijk, beleid en onderwijs." In: N. Kop en P. Tops (red.), *Toestand en toekomst van de opsporing*, Apeldoorn: Politieacademie, 2010, p. 67-134.

Klerks et al. 2002
P.P.H.M. Klerks, C.J.E. in 't Velt, A. Ph. Van Wijk, M.M.E.A. Scholtes, P.S. Nijmeijer en J.G.M. van der Velden, *De voorhoede van de opsporing: Evaluatie van de kernteams als instrument in de aanpak van zware georganiseerde criminaliteit*, Elsevier Overheid, Reed Business Information BV, 2002.

De Kleuver 2007
E.E. de Kleuver, Prestatieafspraken met de politie: van kritiek naar waardering. In: C.J.C.F. Fijnaut, E.R. Muller en U. Rosenthal, *Politie: studies over haar werking en organisatie*, Alphen aan den Rijn: Samson, 1999, p. 213-234.

Knightly 1986
P. Knightly, *The Second Oldest Profession: the spy as patriot, bureaucrat, fantasist and whore*, London: Pan Books, 1986.

Koelewijn 2009
W.I. Koelewijn, *Privacy en politiegegevens: over geautomatiseerde normatieve informatie-uitwisseling*, Leiden: Leiden University Press, 2009.

Koning 2011
M.E. Koning, *Terughacken als opsporingsmethode: een juridische analyse van de terughack praktijk van Justitie in relatie tot het privacyrecht naar aanleiding van de Bredolab ontmanteling*, masterscriptie, Vrije Universiteit, 2011.

Koops, Vedder en Van der Wees 2006
B.J. Koops, Anton Vedder en Leo van der Wees, "Big Brother's bevoegdheden zijn er, nu hij zelf nog?" In: *Nederlands Juristenblad*, 2006, p. 2356-2360.

Kop en Klerks 2009
N. Kop en P. Klerks, *Doctrine Politieacademie: Intelligencegestuurd politiewerk*, Apeldoorn: Politieacademie, 2009.

Kop et al. 2007
N. Kop, T. Derksen, R. Van der Lee en J. Hoekendijk, *Informatie-inwinning in de 'bovenwereld': de wereld op zijn kop*, Apeldoorn: Elsevier Overheid, 2007.

Kramer 2001
R.M. Kramer, "Identity and Trust in Organizations: One Anatomy of a Productive but a Problematic Relationship." In: M.A. Hogg en D.J. Terry (red.), *Social Identity Processes in Organizational Contexts*, Philadelphia: Pscychology Press, Taylor and Francis Group, 2001, p. 167-180.

Vanlandschoot 2005
A. Vanlandschoot, Paneldebat Intelligence Led Policing, 2005. In: Tom Van Den Broeck, Els Enhus, Frank Goegebuer, luc Valkenborg en Annelies Vanlandschoot (ed.), *Intelligence led policing. Definitie, reikwijdte en grenzen*, Brussel: Politeia, 2005, p. 123-138.

Van Lent 2008
L. van Lent, *Externe openbaarheid in het strafproces.* Den Haag: Boom Juridische Uitgevers, 2008.

Lintz 2007
J.M. Lintz, *De plaats van de Wet terroristische misdrijven in het materiële strafrecht: Een onderzoek naar de wederzijdse beïnvloeding door de Wet terroristische misdrijven en het Wetboek van Strafrecht en enkele bijzondere wetten*, Nijmegen: Wolff Legal Publishing, 2007.

Lipsky 1980
M. Lipsky, *Street-level Bureaucracy: dilemmas of the individual in public services*, New York: Russel Sage Foundation, 1980.

Loof 2005
J.P. Loof, *Mensenrechten en staatsveiligheid: verenigbare grootheden?: Opschorting en beperking van mensenrechtenbescherming tijdens noodtoestanden en andere situaties die de staatsveiligheid bedreigen*, Nijmegen: Wolf Legal Publishers, 2005.

Lyon 2006
D. Lyon, "The search for surveillance theories." In: D. Lyon (red.), *Theorizing Surveillance: The panopticon and beyond*, Devon: Willan Publishing, 2006, p. 3-20.

Maas-de Waal 2004
C. Maas-de Waal, "Veiligheid, politie en justitie." In: P. Schnabel, *In het zicht van de toekomst: Sociaal en Cultureel Rapport*, Den Haag: Sociaal Cultureel Planbureau, 2004, p. 457-498.

Maesschalck 2008
J. Maesschalck, "Veranderen van beleid en management in een criminologische context." In: *Panopticon* 29, nr. 2008.5, p. 1-13.

Maguire en John 2006
M. Maguire en T. John, "Intelligence led policing, managerialism and community engagement: competing priorities and the role of the National Intelligence Model in the UK." In: *Policing & Society*, nr. Volume 16, Number 1 (2006), p. 67-85.

Malm, Bichler en Nash 2011
A. Malm, G. Bichler en R. Nash, *Co-offending between criminal enterprise groups.* In: Global Crime Vol. 12, No 2, May 2011, p. 112- 128.

Manning 2005
P.K. Manning, "The police: mandate, strategies, and appearances." In: Tim Newburn (red.), *Policing: Key Readings*, Devon: Willan Publishing, 2005, p. 191-214.

Marx 1974
G.T. Marx, "Thoughts on a Neglected Category of Social Participant: The Agent Provocateur and the Informant." In: *American Journal of Sociology*, nr. Vol. 80, No. 2 (1974), p. 402-442.

McDowell 2009
D. McDowell, *Strategic Intelligence: A Handbook for Practitioners, Managers and Users*, Toronto: The Scarecrow Press, Inc., 2009.

Meesters en Niemeijer 2000
P. Meesters en B. Niemeijer, "Criminaliteitsbeeldanalyse: problemen en mogelijkheden." In: H. Moerland en B. Rovers (red.), *Criminaliteitsanalyse in Nederland*, Den Haag: Elsevier, 2000, p. 293-306.

Meesters, Kortekaas en Trachter 1999
P. Meesters, J. Kortekaas en M. Trachter. "Intelligence led policing: nieuw concept voor integratie van oude adagia." In: *Tijdschrift voor Criminologie*, nr. 41(4) (1999), p. 419-429.

Meeus en Verlaan 2010
J. Meeus en J. Verlaan, "Recherche verruilt intuïtie voor digitaal korset." In: *NRC-Handelsblad*, 9 juni 2010.

Meeus en Haenen 1996
M. Meeus en T.-J. Haenen, *Het IRT moeras*, Amsterdam: Uitgeverij Balans, 1996.

Middelburg en Vugts 2006
B. Middelburg en P. Vugts, *De Endstra-tapes: de integrale gesprekken van Willem Endstra met de recherche*, Amsterdam: Nieuw Amsterdam Uitgevers, 2006.

Minnebo 2004
P. Minnebo, *Criminaliteitsanalyse verklaard: aanzetten voor verdere ontwikkeling van criminaliteitsanalyse*, Den Haag: Elsevier Overheid, 2004.

Moerland en Mooij 2000
H. Moerland en A. Mooij, "Criminaliteitanalyse: een nadere afbakening van het begrip." In: H. Moerland en B. Rovers, *Criminaliteitsanalyse in Nederland*, 's Gravenhage: Elsevier, 2000, p. 33-51.

Morselli 2009
C. Morselli, *Inside criminal networks*. Springer, New York, 2009.

Muller en Petit 2008
E.R. Muller en G.M. Petit, "Strategieën tegen Terrorisme." In: E.R. Muller, U. Rosenthal en R. de Wijk (ed.), *Terrorisme: Studies over Terrorisme en terrorismebestrijding*, Deventer, Kluwer, 2008, p. 271-308

Muller, Rosenthal en de Wijk 2008
E.R. Muller, U. Rosenthal en R. de Wijk (red.), *Terrorisme: Studies over terrorisme en terrorismebestrijding*, Deventer: Kluwer, 2008.

Muller, Spaaij en Ruitenberg 2004
E.R. Muller, R.F.J. Spaaij en A.G.W. Ruitenberg, *Trends in terrorisme*, Deventer: Kluwer, 2004.

Myjer 2002
E. Myjer, "Strafrechtelijk onderzoek en waarheidsvinding." In: *Justitiële Verkenningen (WODC)* 28, nr. 2 02 (2002), p. 26-35.

Nadelmann 1993
E.A. Nadelmann, *Cops Across Borders: The Internalization of U.S. Criminal Law Enforcement*, Pennsylvania: The Pennsylvania State University Press, 1993.

Nonaka 1998
I. Nonaka, "The Knowledge-creating Company." In: *Harvard Business Review on Knowledge Management*, Boston: Harvard Business School Press, 1998, p. , 21-45.

O'Connor 2011
T. O'Connor, "Homeland Security and Law Enforcement", http://www.drtomoconnor.com/3430/3430lect02b.htm, gezien op 05-22-2011

Ogura 2006
T. Ogura, "Electronic government and surveillance-oriented society." In: David Lyon (red.), *Theorizing Surveillance: The panopticon and beyond*, Devon: Willan Publishing, 2006, p. 270-295.

Ontwerpplan Nationale Politie 2011
Kwartiermaker Nationale Politie, *Ontwerpplan Nationale Politie (concept)*, oktober 2011. Niet gepubliceerd.

Peacock 2004
J.L. Peacock, *The Anthropological Lens: Harsh Light, Soft Focus*, Cambridge: Cambridge Press, 2004.

Peters 2001
G.B. Peters, *The Politics of Bureaucracy.* New York: Routledge, 2001.

Posthumus 2005
F. Posthumus, "Evaluatieonderzoek in de Schiedammer Parkmoord." Rapport in opdracht van het College van Procureurs-Generaal, 2005.

Pozen 2005
D. Pozen, "The Mosaic Theory, National Security and Freedom of Information Act." In: *Yale Law Journal*, 2005, p. 628-679.

Punch, Tieleman en van den Berg 1999
M. Punch, P. Tieleman en A.H. van den Berg, "Politiecultuur." In: C.J.C.F. Fijnaut, E.R. Muller en U. Rosenthal, *Politie: studies over haar werking en organisatie*, Alphen aan den Rijn: Samson, 1999, p. 263-282.

Ratcliffe 2008
J. Ratcliffe, *Intelligence Led Policing.* Devon: Willan Publishing, 2008.

Ratcliffe 2009
J. Ratcliffe (red.), *Strategic Thinking in Criminal Intelligence 2nd edition.* Sydney: The Federation Press, 2009.

Rees 2007
L. Rees, *De Nazi´s*. Amsterdam: Ambo/Anthos, 2007.

Reuss-Ianni en Ianni 1983
E. Reuss-Ianni en F.A.J. Ianni. "Street cops and management cops: the two cultures of policing (1983)." In: Tim Newburn, *Policing: Key Readings*, Devon: Willan Publishing, 2005, p. 297-314.

Rosenthal, Muller en Ruitenberg 2006
U. Rosenthal, E. Muller en A. Ruitenberg. *Het terroristische kwaad: diagnose en bestrijding.* Den Haag: Boom Juridische Uitgevers, 2006.

Rosenthal en Van der Torre 2007
U. Rosenthal en E.J. van der Torre, Politiemanagement. In: C.J.C.F. Fijnaut, E.R. Muller en U. Rosenthal, *Politie: studies over haar werking en organisatie*, Alphen aan den Rijn: Samson, 1999, p. 287-312.

Sales 2007
N.A. Sales, "Secrecy and National Security Investigations." In: *Alabama Law Review*, 2007, p. 811-884.

Sales 2010
N.A. Sales, "Share and Share Alike: Intelligence Agencies and Information Sharing." In: *George Washington Law Review*, nr. Vol. 78, No. 2 (February 2010), p. 279-352.

Schermer 2007
B.W. Schermer, *Software agents, surveillance, and the right to privacy: a legislative framework for agent-enabled surveillance.* Leiden: Leiden University Press, 2007.

Schnabel 2004
P. Schnabel, *In het zicht van de toekomst: Sociaal en Cultureel Rapport.* Den Haag: Sociaal en Cultureel Planbureau, 2004.

Scholtes 2009
J.C. Scholtes, "Text mining: de volgende stap in zoektechnologie. Vinden, zonder precies te weten wat men zoekt of vinden wat er niet lijkt te zijn." *Inaugurele Rede.* Maastricht: Océ Business Services, 2009.

Shelby 2002
R.C. Shelby, "September 11 and the Imperative of Reform in the U.S. Intelligence Community: additional views of senator Richard C. Shelby." 2002. Te downloaden van: http://www.fas.org/irp/congress/, gezien op 08-09-2011.

Sheptycki 2004
J. Sheptycki, "Organizational Pathologies in Police Intelligence Systems: Some Contributions to the Lexicon of Intelligence-Led Policing." In: *European Journal of Criminology* Vol. 1, no. 3 (2004), p. 307-332.

Sheptycki 2005
J. Sheptycki, "Transnational Policing." In: *Canadian Review of Policing Research*, 2005 Volume 1.

Sheptycki 2007
J. Sheptycki, "High Policing in the Security Control Society." In: *Policing*, 2007, Volume 1, p. 70-79.

Shils 2009
E. Shils, "Publicity, Privacy and Secrecy: Their Equilibrium and Its Disruption (1956)." In: Susan L. Maret en Jan Goldman (red.), *Government Secrecy: classic and contemporary readings*, London: Libraries Unlimited, 2009, p. 50-58.

Simmel 1906
G. Simmel, "The sociology of secrecy and of secret societies (1906)." In: S.L. Maret en J. Goldman (red.), *Government Secrecy: classic and contemporary readings*, London: Libraries Unlimited, 2009, p. 8-43.

Simon 2007
J. Simon, *Governing Through Crime: How the War on Crime Transformed American Democracy and Created a Culture of Fear.* Oxford: Oxford University Press, 2007.

Sims 2007
J. Sims, "Intelligence to counter terror: the importance of all-source fusion." In: L.K. Johnson (red.), *Strategic Intelligence Volume 4: Counter Intelligence and Counter Terrorism: Defending the Nation Against Hostile Forces*, Westport: Praeger Security International, 2007.

Spapens 2006
T. Spapens, *Interactie tussen criminaliteit en opsporing.* Antwerpen: Intersentia, 2006.

Steele 2007
R. David Steele, "Open source intelligence." In: Loch K. Johnson (red.), *Handbook of intelligence studies*, New York: Routledge, 2007, p. 129-147.

Stol 2007
W.Ph. Stol, "Informatie voor politiewerk: basisprincipes." In: C.J.C.F. Fijnaut, E.R. Muller en U.R. Rosenthal (red.), *Politie: studies over haar werking en organisatie*, Deventer: Kluwer, 2007, p. 381-395.

Stove 2003
R.J. Stove, *The Unsleeping Eye: Secret Police and Their Victims.* San Francisco: Encounter Books, 2003.

Thomas 2009
G. Thomas, *Secret Wars: One Hundred Years of British Intelligence Inside MI5 and MI6*, New York: Thomas Dunne Books, 2009.

Thompson et al. 1998
G. Thompson, J. Frances, R. Levacic en J. Mitchell (red.), *Markets, hierarchies & networks: the coördination of social life.* London: Sage Publications Ltd, 1998.

Van der Torre 2007
E.J. van der Torre, "Politiecultuur." In: C.J.C.F. Fijnaut, E.R. Muller, U. Rosenthal en E.J. Van der Torre (red.), *Politie: Studies over haar werking en organisatie*, Deventer: Kluwer, 2007, p. 495-522.

Van der Torre en Van Harmelen 2007
E.J. van der Torre en E. Van Harmelen, "Basispolitiezorg en hulpverlening." In: C.J.C.F. Fijnaut, E.R. Muller, U. Rosenthal en E.J. Van der Torre (red.), *Politie: Studies over haar werking en organisatie*, Deventer: Kluwer, 2007, p. 917-935.

Van Traa 1996
Van Traa (Parlemtaire Enquete Commissie), "Inzake Opsporing. Eindrapport 1996." Den Haag, 1996.

Turner 2004
M. Turner, *Why secret intelligence fails.* Washington D.C.: Potomac Books Inc., 2004.

Tyler 2001
T. Tyler, "Cooperation in Organizations: A Social Identity Perspective". In: Michael A. Hogg en Deborah J. Terry (red.), *Social Identity Processes in Organizational Contexts*, Philadelphia: Psychology Press, Taylor and Francis Group, 2001,

Van Straelen 2002
Van Straelen, "De informant: inwinnen of opsporen." In: B Andriese en U & J.B.A. de Wit van de Pol (red.), *Criminele informatie: afscherming of openheid?*, Den Haag: Elsevier bedrijfsinformatie, 2002, p. 29-38.

Vedder, Van der Wees en Koops 2006
A.H. Vedder, J.G.L. Van der Wees, en E.J. Koops, "Big Brother's bevoegdheden zijn er - nu hij zelf nog?" In: *Nederlands Juristenblad*, 2006, p. 2356-2360.

Van der Veen 2007
E. van der Veen, "Runners naar school." In: *Blauw*, 3 maart 2007: 25-26.

Versteegh 2005
P. Versteegh, *Informatiegestuurde Veiligheidszorg.* Dordrecht: SMVP, 2005.

Vervaele 2005
J.A.E. Vervaele, "Terrorism and Information Sharing Between the Intelligence and Law Enforcement Communities in the U.S. and the Netherlands: Emergency Criminal Law?" In: A. M. Hol en J.A.E. Vervaele (eds.), *Security and Civil Liberties: The Case of Terrorism*, Utrecht Law Review, Utrecht: Intersentia, 2005, p. 131-165.

Vis 2010
T. Vis, "Het vertrouwen tussen de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de politie: een brug te ver? ." In: R.S.T. Gaarthuis, T. Kooijmans en Th. A. De Roos (red.), *Vertrouwen in de strafrechtspleging*, Deventer: Kluwer, 2010, p. 119-137.

Van der Vijver en Terpstra 2007
C.D. van der Vijver en J.B. Terpstra, "Organisatie en sturing van politiewerk." In: C.J.C.F. Fijnaut, E.R. Muller, U. Rosenthal en E.J. Van der Torre (red.), *Politie: Studies over haar werking en organisatie*, Deventer: Kluwer, 2007, p. 353-380.

Vos et al. 2005
C. Vos, R. Broekhuis, L. Janssen en B. Mounier, *De Geheime Dienst: verhalen over de BVD.* Amsterdam: Boom, 2005.

Vugts 2010
P. Vugts, "Getuige in Holleeder-zaak zegt weinig tot niets." In: *Het Parool*, 30 juni 2010.

Warner 2002
M. Warner, "Wanted: a Definition of Intelligence." In: *Studies in Intelligence* 46, no 3 (2002), p. 15-22.

Weber 1920
M. Weber, "Bureaucracy: Characteristics and the Power Position of Bureaucracy (1920)." In: Susan L. Maret en Jan Goldman, *Government Secrecy: classic and contemporary readings*, London: Libraries Unlimited, 2009, p. 44-49.

Weiner 2007
T. Weiner, *Een spoor van vernieling.* New York: Doubleday, 2007.

Westwood 2001
J. Westwood, "Police Culture and the 'Code of Silence'." 2001. Te downloaden van: *www.opcc.bc.ca*, gezien op 08-09-2011.

Wheaton 2011
K.J. Wheaton, *Sources and Methods.* 20 mei 2011. Te downloaden van: http://www.sourcesandmethods.blogspot.com/ , gezien op 31-05-2011.

Wirtz 2007a
J.J. Wirtz, "The Intelligence-Policy Nexus." In: Loch K. Johnson, *Strategic Intelligence Volume 1: Understanding the Hidden Side of Government*, Westport: Praeger Security International, 2007a, p. 139-150.

Wirtz 2007
J.J. Wirtz, "The American Approach to Intelligence Studies." In: Loch K. Johnson (red.), *Handbook of Intelligence Studies*, New York: Routledge, 2007, p. 28-38.

Van der Woude 2010
M.A.H. van der Woude, *Wetgeving in een Veiligheidscultuur: totstandkoming van antiterrorismewetgeving in Nederland bezien vanuit maatschappelijke en (rechts)politieke context.* Den Haag: Boom Juridische Uitgevers, 2010.

Curriculum Vitae

Thijs Vis is geboren in Delft op 22 september 1980. Hij studeerde rechten aan de Universiteit Utrecht waar hij zich specialiseerde in het strafrecht. Na de rechtenstudie behoorde Thijs tot de eerste lichting van de masterstudie criminologie aan het Willem Pompe Instituut van de Universiteit Utrecht. Tijdens zijn studies is hij bestuurslid van de rechtswinkel van Alphen aan den Rijn geweest en voorzitter van de Utrechtse studievereniging Ad Informandum. Van 2005 tot 2009 heeft hij zich voltijds beziggehouden met zijn promotieonderzoek. In de hoedanigheid van promovendus heeft hij stages gelopen bij het College Bescherming Persoonsgegevens en de politie. Vanaf 2009 is Thijs werkzaam bij de politie.

Thijs heeft zijn promotieonderzoek uitgevoerd bij het Instituut voor Strafrecht en Criminologie aan de Faculteit der Rechtsgeleerdheid van de Universiteit Leiden en de afdeling Strafrechtswetenschappen van de Tilburg Law School van Tilburg University.

SIKS Dissertation Series

1998

1. Johan van den Akker (CWI[306]) *DEGAS - An Active, Temporal Database of Autonomous Objects*
2. Floris Wiesman (UM) *Information Retrieval by Graphically Browsing Meta-Information*
3. Ans Steuten (TUD) *A Contribution to the Linguistic Analysis of Business Conversations within the Language/Action*
4. Dennis Breuker (UM) *Memory versus Search in Games*
5. E.W.Oskamp (RUL) *Computerondersteuning bij Straftoemeting*

1999

1. Mark Sloof (VU) *Physiology of Quality Change Modelling; Automated modelling of Quality Change of Agricultural Products*
2. Rob Potharst (EUR) *Classification using decision trees and neural nets*
3. Don Beal (UM) *The Nature of Minimax Search*
4. Jacques Penders (UM) *The Practical Art of Moving Physical Objects*
5. Aldo de Moor (KUB) *Empowering Communities: A Method for the Legitimate User-Driven Specification of Network Information Systems*
6. Niek J.E. Wijngaards (VU) *Re-design of Compositional Systems*
7. David Spelt (UT) *Verification Support for Object Database Design*
8. Jacques H.J. Lenting (UM) Informed Gambling: *Conception and Analysis of a Multi-Agent Mechanism for Discrete Reallocation*

2000

1. Frank Niessink (VU) *Perspectives on Improving Software Maintenance*
2. Koen Holtman (TU/e) *Prototyping of CMS Storage Management*
3. Carolien M.T. Metselaar (UVA) *Sociaal-organisatorische gevolgen van kennistechnologie; een procesbenadering en actorperspectief*
4. Geert de Haan (VU) *ETAG, A Formal Model of Competence Knowledge for User Interface Design*
5. Ruud van der Pol (UM) *Knowledge-based Query Formulation in Information Retrieval*
6. Rogier van Eijk (UU) *Programming Languages for Agent Communication*
7. Niels Peek (UU) *Decision-theoretic Planning of Clinical Patient Management*
8. Veerle Coupé (EUR) *Sensitivity Analyis of Decision-Theoretic Networks*
9. Florian Waas (CWI) *Principles of Probabilistic Query Optimization*
10. Niels Nes (CWI) *Image Database Management System Design Considerations, Algorithms and Architecture*

[306] Afkortingen: SIKS – Dutch Research School for Information and Knowledge Systems; CWI – Centrum voor Wiskunde en Informatica, Amsterdam; EUR – Erasmus Universiteit, Rotterdam; KUB – Katholieke Universiteit Brabant, Tilburg; KUN - Katholieke Universiteit Nijmegen; OU – Open Universiteit; RUL – Rijksuniversiteit Leiden; RUN – Radbourd Universiteit Nijmegen; TUD – Technische Universiteit Delft; TU/e - Technische Universiteit Eindhoven; UL – Universiteit Leiden; UM – Universiteit Maastricht; UT – Universiteit Twente, Enschede; UU – Universiteit Utrecht; UvA – Universiteit van Amsterdam; UvT – Universiteit van Tilburg; VU – Vrije Universiteit, Amsterdam.

11. Jonas Karlsson (CWI) *Scalable Distributed Data Structures for Database Management*

2001

1. Silja Renooij (UU) *Qualitative Approaches to Quantifying Probabilistic Networks*
2. Koen Hindriks (UU) *Agent Programming Languages: Programming with Mental Models*
3. Maarten van Someren (UvA) *Learning as problem solving*
4. Evgueni Smirnov (UM) *Conjunctive and Disjunctive Version Spaces with Instance-Based Boundary Sets*
5. Jacco van Ossenbruggen (VU) *Processing Structured Hypermedia: A Matter of Style*
6. Martijn van Welie (VU) *Task-based User Interface Design*
7. Bastiaan Schonhage (VU) *Diva: Architectural Perspectives on Information Visualization*
8. Pascal van Eck (VU) *A Compositional Semantic Structure for Multi-Agent Systems Dynamics*
9. Pieter Jan 't Hoen (RUL) *Towards Distributed Development of Large Object-Oriented Models, Views of Packages as Classes*
10. Maarten Sierhuis (UvA) *Modeling and Simulating Work Practice BRAHMS: a multiagent modeling and simulation language for work practice analysis and design*
11. Tom M. van Engers (VUA) Knowledge Management: *The Role of Mental Models in Business Systems Design*

2002

1. Nico Lassing (VU) *Architecture-Level Modifiability Analysis*
2. Roelof van Zwol (UT) *Modelling and searching web-based document collections*
3. Henk Ernst Blok (UT) *Database Optimization Aspects for Information Retrieval*
4. Juan Roberto Castelo Valdueza (UU) *The Discrete Acyclic Digraph Markov Model in Data Mining*
5. Radu Serban (VU) *The Private Cyberspace Modeling Electronic Environments inhabited by Privacy-concerned Agents*
6. Laurens Mommers (UL) *Applied legal epistemology; Building a knowledge-based ontology of the legal domain*
7. Peter Boncz (CWI) *Monet: A Next-Generation DBMS Kernel For Query-Intensive Applications*
8. Jaap Gordijn (VU) *Value Based Requirements Engineering: Exploring Innovative E-Commerce Ideas*
9. Willem-Jan van den Heuvel(KUB) *Integrating Modern Business Applications with Objectified Legacy Systems*
10. Brian Sheppard (UM) *Towards Perfect Play of Scrabble*
11. Wouter C.A. Wijngaards (VU) *Agent Based Modelling of Dynamics: Biological and Organisational Applications*
12. Albrecht Schmidt (Uva) *Processing XML in Database Systems*
13. Hongjing Wu (TU/e) *A Reference Architecture for Adaptive Hypermedia Applications*
14. Wieke de Vries (UU) *Agent Interaction: Abstract Approaches to Modelling, Programming and Verifying Multi-Agent Systems*
15. Rik Eshuis (UT) *Semantics and Verification of UML Activity Diagrams for Workflow Modelling*

16. Pieter van Langen (VU) *The Anatomy of Design: Foundations, Models and Applications*
17. Stefan Manegold (UVA) *Understanding, Modeling, and Improving Main-Memory Database Performance*

2003

1. Heiner Stuckenschmidt (VU) *Ontology-Based Information Sharing in Weakly Structured Environments*
2. Jan Broersen (VU) *Modal Action Logics for Reasoning About Reactive Systems*
3. Martijn Schuemie (TUD) *Human-Computer Interaction and Presence in Virtual Reality Exposure Therapy*
4. Milan Petkovic (UT) *Content-Based Video Retrieval Supported by Database Technology*
5. Jos Lehmann (UVA) *Causation in Artificial Intelligence and Law - A modelling approach*
6. Boris van Schooten (UT) *Development and specification of virtual environments*
7. Machiel Jansen (UvA) *Formal Explorations of Knowledge Intensive Tasks*
8. Yongping Ran (UM) *Repair Based Scheduling*
9. Rens Kortmann (UM) *The resolution of visually guided behaviour*
10. Andreas Lincke (UvT) *Electronic Business Negotiation: Some experimental studies on the interaction between medium, innovation context and culture*
11. Simon Keizer (UT) *Reasoning under Uncertainty in Natural Language Dialogue using Bayesian Networks*
12. Roeland Ordelman (UT) *Dutch speech recognition in multimedia information retrieval*
13. Jeroen Donkers (UM) *Nosce Hostem - Searching with Opponent Models*
14. Stijn Hoppenbrouwers (KUN) *Freezing Language: Conceptualisation Processes across ICT-Supported Organisations*
15. Mathijs de Weerdt (TUD) *Plan Merging in Multi-Agent Systems*
16. Menzo Windhouwer (CWI) *Feature Grammar Systems - Incremental Maintenance of Indexes to Digital Media Warehouses*
17. David Jansen (UT) *Extensions of Statecharts with Probability, Time, and Stochastic Timing*
18. Levente Kocsis (UM) *Learning Search Decisions*

2004

1. Virginia Dignum (UU) *A Model for Organizational Interaction: Based on Agents, Founded in Logic*
2. Lai Xu (UvT) *Monitoring Multi-party Contracts for E-business*
3. Perry Groot (VU) *A Theoretical and Empirical Analysis of Approximation in Symbolic Problem Solving*
4. Chris van Aart (UVA) *Organizational Principles for Multi-Agent Architectures*
5. Viara Popova (EUR) *Knowledge discovery and monotonicity*
6. Bart-Jan Hommes (TUD) *The Evaluation of Business Process Modeling Techniques*
7. Elise Boltjes (UM) *Voorbeeldig onderwijs; voorbeeldgestuurd onderwijs, een opstap naar abstract denken, vooral voor meisjes*
8. Joop Verbeek (UM) *Politie en de Nieuwe Internationale Informatiemarkt, Grensregionale politiële gegevensuitwisseling en digitale expertise*
9. Martin Caminada (VU) *For the Sake of the Argument; explorations into argument-based reasoning*

10. Suzanne Kabel (UVA) *Knowledge-rich indexing of learning-objects*
11. Michel Klein (VU) *Change Management for Distributed Ontologies*
12. The Duy Bui (UT) *Creating emotions and facial expressions for embodied agents*
13. Wojciech Jamroga (UT) *Using Multiple Models of Reality: On Agents who Know how to Play*
14. Paul Harrenstein (UU) *Logic in Conflict. Logical Explorations in Strategic Equilibrium*
15. Arno Knobbe (UU) *Multi-Relational Data Mining*
16. Federico Divina (VU) *Hybrid Genetic Relational Search for Inductive Learning*
17. Mark Winands (UM) *Informed Search in Complex Games*
18. Vania Bessa Machado (UvA) *Supporting the Construction of Qualitative Knowledge Models*
19. Thijs Westerveld (UT) *Using generative probabilistic models for multimedia retrieval*
20. Madelon Evers (Nyenrode) *Learning from Design: facilitating multidisciplinary design teams*

2005

1. Floor Verdenius (UVA) *Methodological Aspects of Designing Induction-Based Applications*
2. Erik van der Werf (UM) *AI techniques for the game of Go*
3. Franc Grootjen (RUN) *A Pragmatic Approach to the Conceptualisation of Language*
4. Nirvana Meratnia (UT) *Towards Database Support for Moving Object data*
5. Gabriel Infante-Lopez (UVA) *Two-Level Probabilistic Grammars for Natural Language Parsing*
6. Pieter Spronck (UM) *Adaptive Game AI*
7. Flavius Frasincar (TU/e) *Hypermedia Presentation Generation for Semantic Web Information Systems*
8. Richard Vdovjak (TU/e) *A Model-driven Approach for Building Distributed Ontology-based Web Applications*
9. Jeen Broekstra (VU) *Storage, Querying and Inferencing for Semantic Web Languages*
10. Anders Bouwer (UVA) *Explaining Behaviour: Using Qualitative Simulation in Interactive Learning Environments*
11. Elth Ogston (VU) *Agent Based Matchmaking and Clustering - A Decentralized Approach to Search*
12. Csaba Boer (EUR) *Distributed Simulation in Industry*
13. Fred Hamburg (UL) *Een Computermodel voor het Ondersteunen van Euthanasiebeslissingen*
14. Borys Omelayenko (VU) *Web-Service configuration on the Semantic Web; Exploring how semantics meets pragmatics*
15. Tibor Bosse (VU) *Analysis of the Dynamics of Cognitive Processes*
16. Joris Graaumans (UU) *Usability of XML Query Languages*
17. Boris Shishkov (TUD) *Software Specification Based on Re-usable Business Components*
18. Danielle Sent (UU) *Test-selection strategies for probabilistic networks*
19. Michel van Dartel (UM) *Situated Representation*
20. Cristina Coteanu (UL) *Cyber Consumer Law, State of the Art and Perspectives*

21. Wijnand Derks (UT) *Improving Concurrency and Recovery in Database Systems by Exploiting Application Semantics*

2006

1. Samuil Angelov (TU/e) *Foundations of B2B Electronic Contracting*
2. Cristina Chisalita (VU) *Contextual issues in the design and use of information technology in organizations*
3. Noor Christoph (UVA) *The role of metacognitive skills in learning to solve problems*
4. Marta Sabou (VU) *Building Web Service Ontologies*
5. Cees Pierik (UU) *Validation Techniques for Object-Oriented Proof Outlines*
6. Ziv Baida (VU) *Software-aided Service Bundling - Intelligent Methods & Tools for Graphical Service Modeling*
7. Marko Smiljanic (UT) *XML schema matching -- balancing efficiency and effectiveness by means of clustering*
8. Eelco Herder (UT) *Forward, Back and Home Again - Analyzing User Behavior on the Web*
9. Mohamed Wahdan (UM) *Automatic Formulation of the Auditor's Opinion*
10. Ronny Siebes (VU) *Semantic Routing in Peer-to-Peer Systems*
11. Joeri van Ruth (UT) *Flattening Queries over Nested Data Types*
12. Bert Bongers (VU) *Interactivation - Towards an e-cology of people, our technological environment, and the arts*
13. Henk-Jan Lebbink (UU) *Dialogue and Decision Games for Information Exchanging Agents*
14. Johan Hoorn (VU) *Software Requirements: Update, Upgrade, Redesign - towards a Theory of Requirements Change*
15. Rainer Malik (UU) *CONAN: Text Mining in the Biomedical Domain*
16. Carsten Riggelsen (UU) *Approximation Methods for Efficient Learning of Bayesian Networks*
17. Stacey Nagata (UU) *User Assistance for Multitasking with Interruptions on a Mobile Device*
18. Valentin Zhizhkun (UVA) *Graph transformation for Natural Language Processing*
19. Birna van Riemsdijk (UU) *Cognitive Agent Programming: A Semantic Approach*
20. Marina Velikova (UvT) *Monotone models for prediction in data mining*
21. Bas van Gils (RUN) *Aptness on the Web*
22. Paul de Vrieze (RUN) *Fundaments of Adaptive Personalisation*
23. Ion Juvina (UU) *Development of Cognitive Model for Navigating on the Web*
24. Laura Hollink (VU) *Semantic Annotation for Retrieval of Visual Resources*
25. Madalina Drugan (UU) *Conditional log-likelihood MDL and Evolutionary MCMC*
26. Vojkan Mihajlovic (UT) *Score Region Algebra: A Flexible Framework for Structured Information Retrieval*
27. Stefano Bocconi (CWI) *Vox Populi: generating video documentaries from semantically annotated media repositories*
28. Borkur Sigurbjornsson (UVA) *Focused Information Access using XML Element Retrieval*

2007

1. Kees Leune (UvT) *Access Control and Service-Oriented Architectures*

2. Wouter Teepe (RUG) *Reconciling Information Exchange and Confidentiality: A Formal Approach*
3. Peter Mika (VU) *Social Networks and the Semantic Web*
4. Jurriaan van Diggelen (UU) *Achieving Semantic Interoperability in Multi-agent Systems: a dialogue-based approach*
5. Bart Schermer (UL) *Software Agents, Surveillance, and the Right to Privacy: a Legislative Framework for Agent-enabled Surveillance*
6. Gilad Mishne (UVA) *Applied Text Analytics for Blogs*
7. Natasa Jovanovic' (UT) *To Whom It May Concern - Addressee Identification in Face-to-Face Meetings*
8. Mark Hoogendoorn (VU) *Modeling of Change in Multi-Agent Organizations*
9. David Mobach (VU) *Agent-Based Mediated Service Negotiation*
10. Huib Aldewereld (UU) *Autonomy vs. Conformity: an Institutional Perspective on Norms and Protocols*
11. Natalia Stash (TU/e) *Incorporating Cognitive/Learning Styles in a General-Purpose Adaptive Hypermedia System*
12. Marcel van Gerven (RUN) *Bayesian Networks for Clinical Decision Support: A Rational Approach to Dynamic Decision-Making under Uncertainty*
13. Rutger Rienks (UT) *Meetings in Smart Environments; Implications of Progressing Technology*
14. Niek Bergboer (UM) *Context-Based Image Analysis*
15. Joyca Lacroix (UM) *NIM: a Situated Computational Memory Model*
16. Davide Grossi (UU) *Designing Invisible Handcuffs. Formal investigations in Institutions and Organizations for Multi-agent Systems*
17. Theodore Charitos (UU) *Reasoning with Dynamic Networks in Practice*
18. Bart Orriens (UvT) *On the development an management of adaptive business collaborations*
19. David Levy (UM) *Intimate relationships with artificial partners*
20. Slinger Jansen (UU) *Customer Configuration Updating in a Software Supply Network*
21. Karianne Vermaas (UU) *Fast diffusion and broadening use: A research on residential adoption and usage of broadband internet in the Netherlands between 2001 and 2005*
22. Zlatko Zlatev (UT) *Goal-oriented design of value and process models from patterns*
23. Peter Barna (TU/e) *Specification of Application Logic in Web Information Systems*
24. Georgina Ramírez Camps (CWI) *Structural Features in XML Retrieval*
25. Joost Schalken (VU) *Empirical Investigations in Software Process Improvement*

2008

1. Katalin Boer-Sorbán (EUR) *Agent-Based Simulation of Financial Markets: A modular, continuous-time approach*
2. Alexei Sharpanskykh (VU) *On Computer-Aided Methods for Modeling and Analysis of Organizations*
3. Vera Hollink (UVA) *Optimizing hierarchical menus: a usage-based approach*
4. Ander de Keijzer (UT) *Management of Uncertain Data - towards unattended integration*
5. Bela Mutschler (UT) *Modeling and simulating causal dependencies on process-aware information systems from a cost perspective*

6. Arjen Hommersom (RUN) *On the Application of Formal Methods to Clinical Guidelines, an Artificial Intelligence Perspective*
7. Peter van Rosmalen (OU) *Supporting the tutor in the design and support of adaptive e-learning*
8. Janneke Bolt (UU) *Bayesian Networks: Aspects of Approximate Inference*
9. Christof van Nimwegen (UU) *The paradox of the guided user: assistance can be counter-effective*
10. Wouter Bosma (UT) *Discourse oriented summarization*
11. Vera Kartseva (VU) *Designing Controls for Network Organizations: A Value-Based Approach*
12. Jozsef Farkas (RUN) *A Semiotically Oriented Cognitive Model of Knowledge Representation*
13. Caterina Carraciolo (UVA) *Topic Driven Access to Scientific Handbooks*
14. Arthur van Bunningen (UT) *Context-Aware Querying; Better Answers with Less Effort*
15. Martijn van Otterlo (UT) *The Logic of Adaptive Behavior: Knowledge Representation and Algorithms for the Markov Decision Process Framework in First-Order Domains*
16. Henriette van Vugt (VU) *Embodied agents from a user's perspective*
17. Martin Op 't Land (TUD) *Applying Architecture and Ontology to the Splitting and Allying of Enterprises*
18. Guido de Croon (UM) *Adaptive Active Vision*
19. Henning Rode (UT) *From Document to Entity Retrieval: Improving Precision and Performance of Focused Text Search*
20. Rex Arendsen (UVA) *Geen bericht, goed bericht. Een onderzoek naar de effecten van de introductie van elektronisch berichtenverkeer met de overheid op de administratieve lasten van bedrijven*
21. Krisztian Balog (UVA) *People Search in the Enterprise*
22. Henk Koning (UU) *Communication of IT-Architecture*
23. Stefan Visscher (UU) *Bayesian network models for the management of ventilator-associated pneumonia*
24. Zharko Aleksovski (VU) *Using background knowledge in ontology matching*
25. Geert Jonker (UU) *Efficient and Equitable Exchange in Air Traffic Management Plan Repair using Spender-signed Currency*
26. Marijn Huijbregts (UT) *Segmentation, Diarization and Speech Transcription: Surprise Data Unraveled*
27. Hubert Vogten (OU) *Design and Implementation Strategies for IMS Learning Design*
28. Ildiko Flesch (RUN) *On the Use of Independence Relations in Bayesian Networks*
29. Dennis Reidsma (UT) *Annotations and Subjective Machines - Of Annotators, Embodied Agents, Users, and Other Humans*
30. Wouter van Atteveldt (VU) *Semantic Network Analysis: Techniques for Extracting, Representing and Querying Media Content*
31. Loes Braun (UM) *Pro-Active Medical Information Retrieval*
32. Trung H. Bui (UT) *Toward Affective Dialogue Management using Partially Observable Markov Decision Processes*
33. Frank Terpstra (UVA) *Scientific Workflow Design; theoretical and practical issues*
34. Jeroen de Knijf (UU) *Studies in Frequent Tree Mining*

35. Ben Torben Nielsen (UvT) *Dendritic morphologies: function shapes structure*

2009

1. Rasa Jurgelenaite (RUN) *Symmetric Causal Independence Models*
2. Willem Robert van Hage (VU) *Evaluating Ontology-Alignment Techniques*
3. Hans Stol (UvT) *A Framework for Evidence-based Policy Making Using IT*
4. Josephine Nabukenya (RUN) *Improving the Quality of Organisational Policy Making using Collaboration Engineering*
5. Sietse Overbeek (RUN) *Bridging Supply and Demand for Knowledge Intensive Tasks - Based on Knowledge, Cognition, and Quality*
6. Muhammad Subianto (UU) *Understanding Classification*
7. Ronald Poppe (UT) *Discriminative Vision-Based Recovery and Recognition of Human Motion*
8. Volker Nannen (VU) *Evolutionary Agent-Based Policy Analysis in Dynamic Environments*
9. Benjamin Kanagwa (RUN) *Design, Discovery and Construction of Service-oriented Systems*
10. Jan Wielemaker (UVA) *Logic programming for knowledge-intensive interactive applications*
11. Alexander Boer (UVA) *Legal Theory, Sources of Law & the Semantic Web*
12. Peter Massuthe (TU/e, Humboldt-Universitaet zu Berlin) *Operating Guidelines for Services*
13. Steven de Jong (UM) *Fairness in Multi-Agent Systems*
14. Maksym Korotkiy (VU) *From ontology-enabled services to service-enabled ontologies (making ontologies work in e-science with ONTO-SOA)*
15. Rinke Hoekstra (UVA) *Ontology Representation - Design Patterns and Ontologies that Make Sense*
16. Fritz Reul (UvT) *New Architectures in Computer Chess*
17. Laurens van der Maaten (UvT) *Feature Extraction from Visual Data*
18. Fabian Groffen (CWI) *Armada, An Evolving Database System*
19. Valentin Robu (CWI) *Modeling Preferences, Strategic Reasoning and Collaboration in Agent-Mediated Electronic Markets*
20. Bob van der Vecht (UU) *Adjustable Autonomy: Controling Influences on Decision Making*
21. Stijn Vanderlooy(UM) *Ranking and Reliable Classification*
22. Pavel Serdyukov (UT) *Search For Expertise: Going beyond direct evidence*
23. Peter Hofgesang (VU) *Modelling Web Usage in a Changing Environment*
24. Annerieke Heuvelink (VU) *Cognitive Models for Training Simulations*
25. Alex van Ballegooij (CWI) *"RAM: Array Database Management through Relational Mapping"*
26. Fernando Koch (UU) *An Agent-Based Model for the Development of Intelligent Mobile Services*
27. Christian Glahn (OU) *Contextual Support of social Engagement and Reflection on the Web*
28. Sander Evers (UT) *Sensor Data Management with Probabilistic Models*
29. Stanislav Pokraev (UT) *Model-Driven Semantic Integration of Service-Oriented Applications*

30. Marcin Zukowski (CWI) *Balancing vectorized query execution with bandwidth-optimized storage*
31. Sofiya Katrenko (UVA) *A Closer Look at Learning Relations from Text*
32. Rik Farenhorst (VU) and Remco de Boer (VU) *Architectural Knowledge Management: Supporting Architects and Auditors*
33. Khiet Truong (UT) *How Does Real Affect Affect Affect Recognition In Speech?*
34. Inge van de Weerd (UU) *Advancing in Software Product Management: An Incremental Method Engineering Approach*
35. Wouter Koelewijn (UL) *Privacy en Politiegegevens; Over geautomatiseerde normatieve informatie-uitwisseling*
36. Marco Kalz (OU) *Placement Support for Learners in Learning Networks*
37. Hendrik Drachsler (OU) *Navigation Support for Learners in Informal Learning Networks*
38. Riina Vuorikari (OU) *Tags and self-organisation: a metadata ecology for learning resources in a multilingual context*
39. Christian Stahl (TU/e, Humboldt-Universitaet zu Berlin) *Service Substitution -- A Behavioral Approach Based on Petri Nets*
40. Stephan Raaijmakers (UvT) *Multinomial Language Learning: Investigations into the Geometry of Language*
41. Igor Berezhnyy (UvT) *Digital Analysis of Paintings*
42. Toine Bogers (UvT) *Recommender Systems for Social Bookmarking*
43. Virginia Nunes Leal Franqueira (UT) *Finding Multi-step Attacks in Computer Networks using Heuristic Search and Mobile Ambients*
44. Roberto Santana Tapia (UT) *Assessing Business-IT Alignment in Networked Organizations*
45. Jilles Vreeken (UU) *Making Pattern Mining Useful*
46. Loredana Afanasiev (UvA) *Querying XML: Benchmarks and Recursion*

2010

1. Matthijs van Leeuwen (UU) *Patterns that Matter*
2. Ingo Wassink (UT) *Work flows in Life Science*
3. Joost Geurts (CWI) *A Document Engineering Model and Processing Framework for Multimedia documents*
4. Olga Kulyk (UT) *Do You Know What I Know? Situational Awareness of Co-located Teams in Multidisplay Environments*
5. Claudia Hauff (UT) *Predicting the Effectiveness of Queries and Retrieval Systems*
6. Sander Bakkes (UvT) *Rapid Adaptation of Video Game AI*
7. Wim Fikkert (UT) *A Gesture interaction at a Distance*
8. Krzysztof Siewicz (UL) *Towards an Improved Regulatory Framework of Free Software. Protecting user freedoms in a world of software communities and eGovernments*
9. Hugo Kielman (UL) *Politiële gegevensverwerking en Privacy, Naar een effectieve waarborging*
10. Rebecca Ong (UL) *Mobile Communication and Protection of Children*
11. Adriaan Ter Mors (TUD) *The world according to MARP: Multi-Agent Route Planning*
12. Susan van den Braak (UU) *Sensemaking software for crime analysis*
13. Gianluigi Folino (RUN) *High Performance Data Mining using Bio-inspired techniques*

14. Sander van Splunter (VU) *Automated Web Service Reconfiguration*
15. Lianne Bodenstaff (UT) *Managing Dependency Relations in Inter-Organizational Models*
16. Sicco Verwer (TUD) *Efficient Identification of Timed Automata, theory and practice*
17. Spyros Kotoulas (VU) *Scalable Discovery of Networked Resources: Algorithms, Infrastructure, Applications*
18. Charlotte Gerritsen (VU) *Caught in the Act: Investigating Crime by Agent-Based Simulation*
19. Henriette Cramer (UvA) *People's Responses to Autonomous and Adaptive Systems*
20. Ivo Swartjes (UT) *Whose Story Is It Anyway? How Improv Informs Agency and Authorship in Emergent Narrative*
21. Harold van Heerde (UT) *Privacy-aware data management by means of data degradation*
22. Michiel Hildebrand (CWI) *End-user Support for Access to\\ Heterogeneous Linked Data*
23. Bas Steunebrink (UU) *The Logical Structure of Emotions*
24. Dmytro Tykhonov (TUD) *Designing Generic and Efficient Negotiation Strategies*
25. Zulfiqar Ali Memon (VU) *Modelling Human-Awareness for Ambient Agents: A Human Mindreading Perspective*
26. Ying Zhang (CWI) *XRPC: Efficient Distributed Query Processing on Heterogeneous XQuery Engines*
27. Marten Voulon (UL) *Automatisch contracteren*
28. Arne Koopman (UU) *Characteristic Relational Patterns*
29. Stratos Idreos (CWI) *Database Cracking: Towards Auto-tuning Database Kernels*
30. Marieke van Erp (UvT) *Accessing Natural History - Discoveries in data cleaning, structuring, and retrieval*
31. Victor de Boer (UVA) *Ontology Enrichment from Heterogeneous Sources on the Web*
32. Marcel Hiel (UvT) *An Adaptive Service Oriented Architecture: Automatically solving Interoperability Problems*
33. Robin Aly (UT) *Modelling Representation Uncertainty in Concept-Based Multimedia Retrieval*
34. Teduh Dirgahayu (UT) *Interaction Design in Service Compositions*
35. Dolf Trieschnigg (UT) *Proof of Concept: Concept-based Biomedical Information Retrieval*
36. Jose Janssen (OU) *Paving the Way for Lifelong Learning; Facilitating competence development through a learning path specification*
37. Niels Lohmann (TU/e) *Correctness of services and their composition*
38. Dirk Fahland (TU/e) *From Scenarios to components*
39. Ghazanfar Farooq Siddiqui (VU) *Integrative modelling of emotions in virtual agents*
40. Mark van Assem (VU) *Converting and Integrating Vocabularies for the Semantic Web*
41. Guillaume Chaslot (UM) *Monte-Carlo Tree Search*
42. Sybren de Kinderen (VU) *Needs-driven service bundling in a multi-supplier setting - the computational e3-service approach*
43. Peter van Kranenburg (UU) *A Computational Approach to Content-Based Retrieval of Folk Song Melodies*
44. Pieter Bellekens (TU/e) *An Approach towards Context-sensitive and User-adapted Access to Heterogeneous Data Sources, Illustrated in the Television Domain*
45. Vasilios Andrikopoulos (UvT) *A theory and model for the evolution of software services*

46. Vincent Pijpers (VU) *e3alignment: Exploring Inter-Organizational Business-ICT Alignment*
47. Chen Li (UT) *Mining Process Model Variants: Challenges, Techniques, Examples*
48. Milan Lovric (EUR) Behavioral Finance and Agent-Based Artificial Markets
49. Jahn-Takeshi Saito (UM) *Solving difficult game positions*
50. Bouke Huurnink (UVA) *Search in Audiovisual Broadcast Archives*
51. Alia Khairia Amin (CWI) *Understanding and supporting information seeking tasks in multiple sources*
52. Peter-Paul van Maanen (VU) *Adaptive Support for Human-Computer Teams: Exploring the Use of Cognitive Models of Trust and Attention*
53. Edgar Meij (UVA) *Combining Concepts and Language Models for Information Access*

2011

1. Botond Cseke (RUN) *Variational Algorithms for Bayesian Inference in Latent Gaussian Models*
2. Nick Tinnemeier (UU) *Organizing Agent Organizations. Syntax and Operational Semantics of an Organization-Oriented Programming Language*
3. Jan Martijn van der Werf (TU/e) *Compositional Design and Verification of Component-Based Information Systems*
4. Hado van Hasselt (UU) *Insights in Reinforcement Learning Formal analysis and empirical evaluation of temporal-difference learning algorithms*
5. Base van der Raadt (VU) *Enterprise Architecture Coming of Age - Increasing the Performance of an Emerging Discipline*
6. Yiwen Wang (TU/e) *Semantically-Enhanced Recommendations in Cultural Heritage*
7. Yujia Cao (UT) *Multimodal Information Presentation for High Load Human Computer Interaction*
8. Nieske Vergunst (UU) *BDI-based Generation of Robust Task-Oriented Dialogues*
9. Tim de Jong (OU) *Contextualised Mobile Media for Learning*
10. Bart Bogaert (TU) *Cloud Content Contention*
11. Dhaval Vyas (UT) *Designing for Awareness: An Experience-focused HCI Perspective*
12. Carmen Bratosin (TU/e) *Grid Architecture for Distributed Process Mining*
13. Xiaoyu Mao (UvT) *Airport under Control. Multiagent Scheduling for Airport Ground Handling*

2012

1. Terry Najja Kakeeto (UvT) *Relationship Marketing for SMEs in Uganda*
2. Muhammad Umair(VU) *Adaptivity, emotion, and Rationality in Human and Ambient Agent Models*
3. Adam Vanya (VU) *Supporting Architecture Evolution by Mining Software Repositories*
4. Jurriaan Souer (UU) *Development of Content Management System-based Web Applications*
5. Marijn Plomp (UU) *Maturing Interorganisational Information Systems*
6. Wolfgang Reinhardt (OU) *Awareness Support for Knowledge Workers in Research Networks*
7. Rianne van Lambalgen (VU) *When the Going Gets Tough: Exploring Agent-based Models of Human Performance under Demanding Conditions*
8. Gerben de Vries (UVA) *Kernel Methods for Vessel Traject*

9. Ricardo Neisse (UT) *Trust and Privacy Management Support for Context-Aware Service Platforms*
10. David Smits (TUE) *Towards a Generic Distributed Adaptive Hypermedia Environment*
11. J.C.B. Rantham Prabhakara (TUE) *Process Mining in the Large: Preprocessing, Discovery, and Diagnostics*
12. Kees van der Sluijs (TUE) *Model Driven Design and Data Integration in Semantic Web Information Systems*
13. Suleman Shahid (UvT) *Fun and Face: Exploring non-verbal expressions of emotion during playful interactions*
14. Evgeny Knutov(TUE) *Generic Adaptation Framework for Unifying Adaptive Web-based Systems*
15. Natalie van der Wal (VU) *Social Agents. Agent-Based Modelling of Integrated Internal and Social Dynamics of Cognitive and Affective Processes.*
16. Fiemke Both (VU) *Helping people by understanding them - Ambient Agents supporting task execution and depression treatment*
17. Amal Elgammal (UvT) *Towards a Comprehensive Framework for Business Process Compliance*
18. Eltjo Poort (VU) *Improving Solution Architecting Practices*
19. Helen Schonenberg (TUE) *What's Next? Operational Support for Business Process Execution*
20. Ali Bahramisharif (RUN) *Covert Visual Spatial Attention, a Robust Paradigm for Brain-Computer Interfacing*
21. Roberto Cornacchia (CWI) *Querying Sparse Matrices for Information Retrieval*
22. Thijs Vis (UvT) *Intelligence, politie en veiligheidsdienst: verenigbare grootheden?*

TiCC Ph.D. Series

1. Pashiera Barkhuysen. *Audiovisual Prosody in Interaction.* Promotores: M.G.J. Swerts, E.J. Krahmer. Tilburg, 3 October 2008.

2. Ben Torben-Nielsen. *Dendritic morphology: function shapes structure.* Promotores: H.J. van den Herik, E.O. Postma. Co-promotor: K.P. Tuyls. Tilburg, 3 December 2008.

3. Hans Stol. *A framework for evidence-based policy making using IT.* Promotor: H.J. van den Herik. Tilburg, 21 January 2009.

4. Jeroen Geertzen. *Dialogue act recognition and prediction.* Promotor: H. Bunt. Co-promotor: J.M.B. Terken. Tilburg, 11 February 2009.

5. Sander Canisius. *Structured prediction for natural language processing.* Promotores: A.P.J. van den Bosch, W. Daelemans. Tilburg, 13 February 2009.

6. Fritz Reul. *New Architectures in Computer Chess.* Promotor: H.J. van den Herik. Co-promotor: J.W.H.M. Uiterwijk. Tilburg, 17 June 2009.

7. Laurens van der Maaten. *Feature Extraction from Visual Data.* Promotores: E.O. Postma, H.J. van den Herik. Co-promotor: A.G. Lange. Tilburg, 23 June 2009 (cum laude).

8. Stephan Raaijmakers. *Multinomial Language Learning.* Promotores: W. Daelemans, A.P.J. van den Bosch. Tilburg, 1 December 2009.

9. Igor Berezhnoy. *Digital Analysis of Paintings.* Promotores: E.O. Postma, H.J. van den Herik. Tilburg, 7 December 2009.

10. Toine Bogers. *Recommender Systems for Social Bookmarking.* Promotor: A.P.J. van den Bosch. Tilburg, 8 December 2009.

11. Sander Bakkes. *Rapid Adaptation of Video Game AI.* Promotor: H.J. van den Herik. Co-promotor: P. Spronck. Tilburg, 3 March 2010.

12. Maria Mos. *Complex Lexical Items.* Promotor: A.P.J. van den Bosch. Co-promotores: A. Vermeer, A. Backus. Tilburg, 12 May 2010 (in collaboration with the Department of Language and Culture Studies).

13. Marieke van Erp: *Accessing Natural History. Discoveries in data cleaning, structuring, and retrieval*. Promotor: A.P.J. van den Bosch. Tilburg, 30 June 2010.

14. Edwin Commandeur: *Implicit Causality and Implicit Consequentiality in Language Comprehension*. Promotores: L.G.M. Noordman, W. Vonk. Co-promotor: R. Cozijn. Tilburg, 30 June 2010.

15. Bart Bogaert: *Cloud Content Contention*. Promotores: H.J. van den Herik, E.O. Postma. Tilburg, 30 March 2011.

16. Xiaoyu Mao: *Airport under Control.* Promotores: H.J. van den Herik, E.O. Postma. Co-promotores: N. Roos, A. Salden. Tilburg, 25 May 2011.

17. Olga Petukhova: *Multidimensional Dialogue Modelling*. Promotor: H. Bunt. Tilburg, 1 September 2011.

18. Lisette Mol: *Language in the Hands.* Promotores: F. Maes, E.J. Krahmer, M.G.J. Swerts. Tilburg, 7 November 2011.

19. Herman Stehouwer: *Statistical Language Models for Alternative Sequence Selection*. Promotores: A.P.J. van den Bosch, H.J. van den Herik. Co-Promotor: M.M. van Zaanen. Tilburg, 7 December 2011.

20. Terry Kakeeto-Aelen: *Relationship Marketing for SMEs in Uganda*. Promotores: J. Chr. van Dalen, H.J. van den Herik. Co-promotor: B. van der Walle. Tilburg, 1 February 2012.

21. Suleman Shahid: *Fun & Face: Exploring non-verbal expressions of emotion during playful interactions*. Promotores: E.J. Krahmer, M.G.J. Swerts. Tilburg, 25 May 2012.

22. Thijs Vis: *Intelligence, politie en veiligheidsdienst: verenigbare grootheden?* Promotores: T.A. de Roos, H.J. van den Herik, A.C.M. Spapens. Tilburg, 6 juni 2012.